Guia de referência

AWS Política gerenciada



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Política gerenciada: Guia de referência

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que são as políticas gerenciadas pela AWS? 1
Compreender as páginas de referência de políticas 1
Políticas gerenciadas pela AWS obsoletas 2
AWS políticas gerenciadas 3
AccessAnalyzerServiceRolePolicy 57
Utilização desta política 57
Detalhes desta política 57
Versão da política 57
Documento da política JSON 58
Saiba mais 60
AccountAccessManagerServiceRolePolicy 60
Utilização desta política 61
Detalhes desta política 61
Versão da política 61
Documento da política JSON 61
Saiba mais 62
AccountManagementFromVercel 62
Utilização desta política 62
Detalhes desta política 62
Versão da política 62
Documento da política JSON 63
Saiba mais 64
AdministratorAccess 64
Utilização desta política 65
Detalhes desta política 65
Versão da política 65
Documento da política JSON 65
Saiba mais 65
AdministratorAccess-Amplify 66
Utilização desta política 66
Detalhes desta política 66
Versão da política 66
Documento da política JSON 66
Saiba mais 77

AdministratorAccess-AWSElasticBeanstalk 77
Utilização desta política 77
Detalhes desta política 77
Versão da política 77
Documento da política JSON 78
Saiba mais 86
AgentRegistryFullAccess 86
Utilização desta política 86
Detalhes desta política 86
Versão da política 87
Documento da política JSON 87
Saiba mais 90
AgentRegistryReadOnlyAccess 91
Utilização desta política 91
Detalhes desta política 91
Versão da política 91
Documento da política JSON 91
Saiba mais 92
AIDevOpsAgentAccessPolicy 92
Utilização desta política 92
Detalhes desta política 92
Versão da política 92
Documento da política JSON 93
Saiba mais 115
AIDevOpsAgentActionsPolicy 116
Utilização desta política 116
Detalhes desta política 116
Versão da política 116
Documento da política JSON 116
Saiba mais 117
AIDevOpsAgentFullAccess 117
Utilização desta política 118
Detalhes desta política 118
Versão da política 118
Documento da política JSON 118
Saiba mais 120

AIDevOpsAgentReadOnlyAccess 121
Utilização desta política 121
Detalhes desta política 121
Versão da política 121
Documento da política JSON 121
Saiba mais 122
AIDevOpsChannelAccessPolicy 122
Utilização desta política 122
Detalhes desta política 122
Versão da política 122
Documento da política JSON 123
Saiba mais 123
AIDevOpsConstellationAccessPolicy 123
Utilização desta política 124
Detalhes desta política 124
Versão da política 124
Documento da política JSON 124
Saiba mais 125
AIDevOpsOperatorAppAccessPolicy 125
Utilização desta política 125
Detalhes desta política 125
Versão da política 125
Documento da política JSON 126
Saiba mais 129
AIDevOpsReleaseManagementVPCPolicy 129
Utilização desta política 129
Detalhes desta política 129
Versão da política 129
Documento da política JSON 130
Saiba mais 132
AIOpsAssistantIncidentReportPolicy 133
Utilização desta política 133
Detalhes desta política 133
Versão da política 133
Documento da política JSON 133
Saiba mais 134

AIOpsAssistantPolicy 134
Utilização desta política 135
Detalhes desta política 135
Versão da política 135
Documento da política JSON 135
Saiba mais 156
AIOpsConsoleAdminPolicy 156
Utilização desta política 156
Detalhes desta política 156
Versão da política 156
Documento da política JSON 157
Saiba mais 163
AIOpsOperatorAccess 163
Utilização desta política 163
Detalhes desta política 163
Versão da política 163
Documento da política JSON 164
Saiba mais 166
AIOpsReadOnlyAccess 167
Utilização desta política 167
Detalhes desta política 167
Versão da política 167
Documento da política JSON 167
Saiba mais 168
AlexaForBusinessDeviceSetup 168
Utilização desta política 168
Detalhes desta política 168
Versão da política 169
Documento da política JSON 169
Saiba mais 169
AlexaForBusinessFullAccess 170
Utilização desta política 170
Detalhes desta política 170
Versão da política 170
Documento da política JSON 170
Saiba mais 172

AlexaForBusinessGatewayExecution 172
Utilização desta política 172
Detalhes desta política 172
Versão da política 172
Documento da política JSON 173
Saiba mais 173
AlexaForBusinessLifesizeDelegatedAccessPolicy 174
Utilização desta política 174
Detalhes desta política 174
Versão da política 174
Documento da política JSON 174
Saiba mais 177
AlexaForBusinessNetworkProfileServicePolicy 177
Utilização desta política 177
Detalhes desta política 177
Versão da política 177
Documento da política JSON 178
Saiba mais 178
AlexaForBusinessPolyDelegatedAccessPolicy 178
Utilização desta política 179
Detalhes desta política 179
Versão da política 179
Documento da política JSON 179
Saiba mais 181
AlexaForBusinessReadOnlyAccess 181
Utilização desta política 181
Detalhes desta política 181
Versão da política 181
Documento da política JSON 182
Saiba mais 182
AmazonAPIGatewayAdministrator 182
Utilização desta política 182
Detalhes desta política 183
Versão da política 183
Documento da política JSON 183
Saiba mais 183

AmazonAPIGatewayInvokeFullAccess 184
Utilização desta política 184
Detalhes desta política 184
Versão da política 184
Documento da política JSON 184
Saiba mais 185
AmazonAPIGatewayPushToCloudWatchLogs 185
Utilização desta política 185
Detalhes desta política 185
Versão da política 185
Documento da política JSON 185
Saiba mais 186
AmazonAppFlowFullAccess 186
Utilização desta política 186
Detalhes desta política 186
Versão da política 187
Documento da política JSON 187
Saiba mais 190
AmazonAppFlowReadOnlyAccess 190
Utilização desta política 190
Detalhes desta política 190
Versão da política 190
Documento da política JSON 190
Saiba mais 191
AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy 191
Utilização desta política 191
Detalhes desta política 191
Versão da política 192
Documento da política JSON 192
Saiba mais 193
AmazonAppStreamFullAccess 193
Utilização desta política 194
Detalhes desta política 194
Versão da política 194
Documento da política JSON 194
Saiba mais 196

AmazonAppStreamPCAAccess 196
Utilização desta política 196
Detalhes desta política 196
Versão da política 197
Documento da política JSON 197
Saiba mais 197
AmazonAppStreamReadOnlyAccess 198
Utilização desta política 198
Detalhes desta política 198
Versão da política 198
Documento da política JSON 198
Saiba mais 199
AmazonAppStreamServiceAccess 199
Utilização desta política 199
Detalhes desta política 199
Versão da política 199
Documento da política JSON 200
Saiba mais 201
AmazonAthenaFullAccess 201
Utilização desta política 201
Detalhes desta política 201
Versão da política 201
Documento da política JSON 202
Saiba mais 205
AmazonAthenaServiceRolePolicy 205
Utilização desta política 205
Detalhes desta política 206
Versão da política 206
Documento da política JSON 206
Saiba mais 207
AmazonAugmentedAIFullAccess 207
Utilização desta política 207
Detalhes desta política 207
Versão da política 207
Documento da política JSON 207
Saiba mais 208

AmazonAugmentedAIHumanLoopFullAccess 209
Utilização desta política 209
Detalhes desta política 209
Versão da política 209
Documento da política JSON 209
Saiba mais 210
AmazonAugmentedAIIntegratedAPIAccess 210
Utilização desta política 210
Detalhes desta política 210
Versão da política 210
Documento da política JSON 211
Saiba mais 212
AmazonAuroraDSQLConsoleFullAccess 212
Utilização desta política 212
Detalhes desta política 212
Versão da política 213
Documento da política JSON 213
Saiba mais 215
AmazonAuroraDSQLFullAccess 215
Utilização desta política 216
Detalhes desta política 216
Versão da política 216
Documento da política JSON 216
Saiba mais 219
AmazonAuroraDSQLReadOnlyAccess 219
Utilização desta política 219
Detalhes desta política 219
Versão da política 219
Documento da política JSON 220
Saiba mais 220
AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy 221
Utilização desta política 221
Detalhes desta política 221
Versão da política 221
Documento da política JSON 221
Saiba mais 222

AmazonBedrockExternalWebSearchFullAccess 223
Utilização desta política 223
Detalhes desta política 223
Versão da política 223
Documento da política JSON 223
Saiba mais 224
AmazonBedrockExternalWebSearchReadOnly 224
Utilização desta política 224
Detalhes desta política 224
Versão da política 224
Documento da política JSON 225
Saiba mais 225
AmazonBedrockFullAccess 225
Utilização desta política 225
Detalhes desta política 226
Versão da política 226
Documento da política JSON 226
Saiba mais 231
AmazonBedrockLimitedAccess 232
Utilização desta política 232
Detalhes desta política 232
Versão da política 232
Documento da política JSON 232
Saiba mais 235
AmazonBedrockMantleFullAccess 235
Utilização desta política 235
Detalhes desta política 235
Versão da política 236
Documento da política JSON 236
Saiba mais 237
AmazonBedrockMantleInferenceAccess 237
Utilização desta política 237
Detalhes desta política 237
Versão da política 237
Documento da política JSON 238
Saiba mais 239

AmazonBedrockMantleReadOnly 239
Utilização desta política 239
Detalhes desta política 239
Versão da política 239
Documento da política JSON 240
Saiba mais 240
AmazonBedrockMarketplaceAccess 240
Utilização desta política 241
Detalhes desta política 241
Versão da política 241
Documento da política JSON 241
Saiba mais 245
AmazonBedrockReadOnly 246
Utilização desta política 246
Detalhes desta política 246
Versão da política 246
Documento da política JSON 246
Saiba mais 248
AmazonBedrockStudioPermissionsBoundary 248
Utilização desta política 248
Detalhes desta política 248
Versão da política 248
Documento da política JSON 248
Saiba mais 253
AmazonBedrockWebSearchFullAccess 253
Utilização desta política 253
Detalhes desta política 253
Versão da política 253
Documento da política JSON 253
Saiba mais 254
AmazonBedrockWebSearchReadOnly 254
Utilização desta política 254
Detalhes desta política 254
Versão da política 255
Documento da política JSON 255
Saiba mais 255

AmazonBioDiscoveryFullAccess 255
Utilização desta política 256
Detalhes desta política 256
Versão da política 256
Documento da política JSON 256
Saiba mais 259
AmazonBioDiscoveryInAppFullAccess 259
Utilização desta política 259
Detalhes desta política 259
Versão da política 259
Documento da política JSON 260
Saiba mais 261
AmazonBraketFullAccess 262
Utilização desta política 262
Detalhes desta política 262
Versão da política 262
Documento da política JSON 262
Saiba mais 267
AmazonBraketJobsExecutionPolicy 267
Utilização desta política 267
Detalhes desta política 267
Versão da política 268
Documento da política JSON 268
Saiba mais 271
AmazonBraketServiceRolePolicy 271
Utilização desta política 271
Detalhes desta política 271
Versão da política 271
Documento da política JSON 272
Saiba mais 273
AmazonChimeFullAccess 273
Utilização desta política 273
Detalhes desta política 273
Versão da política 273
Documento da política JSON 274
Saiba mais 276

AmazonChimeReadOnly 276
Utilização desta política 276
Detalhes desta política 276
Versão da política 276
Documento da política JSON 277
Saiba mais 277
AmazonChimeSDK 277
Utilização desta política 277
Detalhes desta política 277
Versão da política 278
Documento da política JSON 278
Saiba mais 279
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy 279
Utilização desta política 279
Detalhes desta política 279
Versão da política 280
Documento da política JSON 280
Saiba mais 281
AmazonChimeSDKMessagingServiceRolePolicy 281
Utilização desta política 281
Detalhes desta política 282
Versão da política 282
Documento da política JSON 282
Saiba mais 283
AmazonChimeServiceRolePolicy 283
Utilização desta política 283
Detalhes desta política 283
Versão da política 283
Documento da política JSON 284
Saiba mais 284
AmazonChimeTranscriptionServiceLinkedRolePolicy 284
Utilização desta política 285
Detalhes desta política 285
Versão da política 285
Documento da política JSON 285
Saiba mais 286

AmazonChimeUserManagement 286
Utilização desta política 286
Detalhes desta política 286
Versão da política 286
Documento da política JSON 286
Saiba mais 288
AmazonChimeVoiceConnectorServiceLinkedRolePolicy 288
Utilização desta política 288
Detalhes desta política 288
Versão da política 288
Documento da política JSON 289
Saiba mais 290
AmazonCloudDirectoryFullAccess 290
Utilização desta política 291
Detalhes desta política 291
Versão da política 291
Documento da política JSON 291
Saiba mais 292
AmazonCloudDirectoryReadOnlyAccess 292
Utilização desta política 292
Detalhes desta política 292
Versão da política 292
Documento da política JSON 292
Saiba mais 293
AmazonCloudWatchEvidentlyFullAccess 293
Utilização desta política 293
Detalhes desta política 293
Versão da política 294
Documento da política JSON 294
Saiba mais 296
AmazonCloudWatchEvidentlyReadOnlyAccess 296
Utilização desta política 297
Detalhes desta política 297
Versão da política 297
Documento da política JSON 297
Saiba mais 298

AmazonCloudWatchEvidentlyServiceRolePolicy 298
Utilização desta política 298
Detalhes desta política 298
Versão da política 298
Documento da política JSON 299
Saiba mais 300
AmazonCloudWatchRUMFullAccess 300
Utilização desta política 300
Detalhes desta política 300
Versão da política 301
Documento da política JSON 301
Saiba mais 303
AmazonCloudWatchRUMReadOnlyAccess 303
Utilização desta política 304
Detalhes desta política 304
Versão da política 304
Documento da política JSON 304
Saiba mais 305
AmazonCloudWatchRUMServiceRolePolicy 306
Utilização desta política 306
Detalhes desta política 306
Versão da política 306
Documento da política JSON 306
Saiba mais 307
AmazonCodeCatalystFullAccess 307
Utilização desta política 307
Detalhes desta política 308
Versão da política 308
Documento da política JSON 308
Saiba mais 309
AmazonCodeCatalystReadOnlyAccess 309
Utilização desta política 309
Detalhes desta política 309
Versão da política 309
Documento da política JSON 310
Saiba mais 310

AmazonCodeCatalystSupportAccess 310
Utilização desta política 310
Detalhes desta política 311
Versão da política 311
Documento da política JSON 311
Saiba mais 312
AmazonCodeGuruProfilerAgentAccess 312
Utilização desta política 312
Detalhes desta política 312
Versão da política 312
Documento da política JSON 313
Saiba mais 313
AmazonCodeGuruProfilerFullAccess 313
Utilização desta política 313
Detalhes desta política 313
Versão da política 314
Documento da política JSON 314
Saiba mais 315
AmazonCodeGuruProfilerReadOnlyAccess 315
Utilização desta política 315
Detalhes desta política 315
Versão da política 315
Documento da política JSON 315
Saiba mais 316
AmazonCodeGuruReviewerFullAccess 316
Utilização desta política 316
Detalhes desta política 316
Versão da política 317
Documento da política JSON 317
Saiba mais 319
AmazonCodeGuruReviewerReadOnlyAccess 320
Utilização desta política 320
Detalhes desta política 320
Versão da política 320
Documento da política JSON 320
Saiba mais 321

AmazonCodeGuruReviewerServiceRolePolicy 321
Utilização desta política 321
Detalhes desta política 321
Versão da política 321
Documento da política JSON 322
Saiba mais 324
AmazonCodeGuruSecurityFullAccess 324
Utilização desta política 324
Detalhes desta política 324
Versão da política 324
Documento da política JSON 324
Saiba mais 325
AmazonCodeGuruSecurityScanAccess 325
Utilização desta política 325
Detalhes desta política 325
Versão da política 326
Documento da política JSON 326
Saiba mais 326
AmazonCognitoDeveloperAuthenticatedIdentities 326
Utilização desta política 327
Detalhes desta política 327
Versão da política 327
Documento da política JSON 327
Saiba mais 328
AmazonCognitoIdpEmailServiceRolePolicy 328
Utilização desta política 328
Detalhes desta política 328
Versão da política 328
Documento da política JSON 329
Saiba mais 329
AmazonCognitoIdpServiceRolePolicy 329
Utilização desta política 329
Detalhes desta política 330
Versão da política 330
Documento da política JSON 330
Saiba mais 330

AmazonCognitoPowerUser 331
Utilização desta política 331
Detalhes desta política 331
Versão da política 331
Documento da política JSON 331
Saiba mais 333
AmazonCognitoReadOnly 333
Utilização desta política 333
Detalhes desta política 333
Versão da política 333
Documento da política JSON 333
Saiba mais 334
AmazonCognitoUnAuthedIdentitiesSessionPolicy 334
Utilização desta política 335
Detalhes desta política 335
Versão da política 335
Documento da política JSON 335
Saiba mais 336
AmazonCognitoUnauthenticatedIdentities 336
Utilização desta política 337
Detalhes desta política 337
Versão da política 337
Documento da política JSON 337
Saiba mais 338
AmazonConnect_FullAccess 338
Utilização desta política 338
Detalhes desta política 338
Versão da política 338
Documento da política JSON 339
Saiba mais 341
AmazonConnectCampaignsServiceLinkedRolePolicy 341
Utilização desta política 342
Detalhes desta política 342
Versão da política 342
Documento da política JSON 342
Saiba mais 346

AmazonConnectReadOnlyAccess 346
Utilização desta política 346
Detalhes desta política 346
Versão da política 346
Documento da política JSON 346
Saiba mais 347
AmazonConnectServiceLinkedRolePolicy 347
Utilização desta política 347
Detalhes desta política 347
Versão da política 348
Documento da política JSON 348
Saiba mais 357
AmazonConnectSynchronizationServiceRolePolicy 357
Utilização desta política 357
Detalhes desta política 357
Versão da política 357
Documento da política JSON 357
Saiba mais 359
AmazonConnectVoiceIDFullAccess 359
Utilização desta política 360
Detalhes desta política 360
Versão da política 360
Documento da política JSON 360
Saiba mais 360
AmazonDataZoneBedrockModelConsumptionPolicy 361
Utilização desta política 361
Detalhes desta política 361
Versão da política 361
Documento da política JSON 361
Saiba mais 364
AmazonDataZoneBedrockModelManagementPolicy 364
Utilização desta política 364
Detalhes desta política 364
Versão da política 364
Documento da política JSON 365
Saiba mais 366

AmazonDataZoneDomainExecutionRolePolicy 367
Utilização desta política 367
Detalhes desta política 367
Versão da política 367
Documento da política JSON 367
Saiba mais 371
AmazonDataZoneEnvironmentRolePermissionsBoundary 371
Utilização desta política 371
Detalhes desta política 371
Versão da política 372
Documento da política JSON 372
Saiba mais 385
AmazonDataZoneFullAccess 385
Utilização desta política 385
Detalhes desta política 385
Versão da política 385
Documento da política JSON 386
Saiba mais 394
AmazonDataZoneFullUserAccess 395
Utilização desta política 395
Detalhes desta política 395
Versão da política 395
Documento da política JSON 395
Saiba mais 399
AmazonDataZoneGlueManageAccessRolePolicy 399
Utilização desta política 399
Detalhes desta política 399
Versão da política 400
Documento da política JSON 400
Saiba mais 407
AmazonDataZonePortalFullAccessPolicy 408
Utilização desta política 408
Detalhes desta política 408
Versão da política 408
Documento da política JSON 408
Saiba mais 409

AmazonDataZonePreviewConsoleFullAccess 409
Utilização desta política 409
Detalhes desta política 409
Versão da política 409
Documento da política JSON 410
Saiba mais 411
AmazonDataZoneProjectDeploymentPermissionsBoundary 412
Utilização desta política 412
Detalhes desta política 412
Versão da política 412
Documento da política JSON 412
Saiba mais 420
AmazonDataZoneProjectRolePermissionsBoundary 421
Utilização desta política 421
Detalhes desta política 421
Versão da política 421
Documento da política JSON 421
Saiba mais 428
AmazonDataZoneRedshiftGlueProvisioningPolicy 429
Utilização desta política 429
Detalhes desta política 429
Versão da política 429
Documento da política JSON 429
Saiba mais 437
AmazonDataZoneRedshiftManageAccessRolePolicy 437
Utilização desta política 437
Detalhes desta política 438
Versão da política 438
Documento da política JSON 438
Saiba mais 441
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 441
Utilização desta política 442
Detalhes desta política 442
Versão da política 442
Documento da política JSON 442
Saiba mais 470

AmazonDataZoneSageMakerManageAccessRolePolicy 470
Utilização desta política 470
Detalhes desta política 470
Versão da política 470
Documento da política JSON 471
Saiba mais 475
AmazonDataZoneSageMakerProvisioningRolePolicy 475
Utilização desta política 476
Detalhes desta política 476
Versão da política 476
Documento da política JSON 476
Saiba mais 481
AmazonDetectiveFullAccess 481
Utilização desta política 481
Detalhes desta política 481
Versão da política 481
Documento da política JSON 482
Saiba mais 483
AmazonDetectiveInvestigatorAccess 483
Utilização desta política 483
Detalhes desta política 483
Versão da política 483
Documento da política JSON 484
Saiba mais 485
AmazonDetectiveMemberAccess 485
Utilização desta política 485
Detalhes desta política 486
Versão da política 486
Documento da política JSON 486
Saiba mais 486
AmazonDetectiveOrganizationsAccess 487
Utilização desta política 487
Detalhes desta política 487
Versão da política 487
Documento da política JSON 487
Saiba mais 489

AmazonDetectiveServiceLinkedRolePolicy 489
Utilização desta política 489
Detalhes desta política 490
Versão da política 490
Documento da política JSON 490
Saiba mais 490
AmazonDevOpsGuruConsoleFullAccess 491
Utilização desta política 491
Detalhes desta política 491
Versão da política 491
Documento da política JSON 491
Saiba mais 494
AmazonDevOpsGuruFullAccess 494
Utilização desta política 494
Detalhes desta política 494
Versão da política 494
Documento da política JSON 494
Saiba mais 497
AmazonDevOpsGuruOrganizationsAccess 497
Utilização desta política 497
Detalhes desta política 497
Versão da política 497
Documento da política JSON 498
Saiba mais 499
AmazonDevOpsGuruReadOnlyAccess 499
Utilização desta política 499
Detalhes desta política 499
Versão da política 499
Documento da política JSON 500
Saiba mais 502
AmazonDevOpsGuruServiceRolePolicy 502
Utilização desta política 502
Detalhes desta política 502
Versão da política 502
Documento da política JSON 503
Saiba mais 507

AmazonDMSCloudWatchLogsRole 507
Utilização desta política 507
Detalhes desta política 507
Versão da política 507
Documento da política JSON 507
Saiba mais 509
AmazonDMSRedshiftS3Role 509
Utilização desta política 509
Detalhes desta política 509
Versão da política 510
Documento da política JSON 510
Saiba mais 510
AmazonDMSVPCManagementRole 511
Utilização desta política 511
Detalhes desta política 511
Versão da política 511
Documento da política JSON 511
Saiba mais 512
AmazonDocDB-ElasticServiceRolePolicy 512
Utilização desta política 512
Detalhes desta política 512
Versão da política 513
Documento da política JSON 513
Saiba mais 513
AmazonDocDBConsoleFullAccess 514
Utilização desta política 514
Detalhes desta política 514
Versão da política 514
Documento da política JSON 514
Saiba mais 519
AmazonDocDBElasticFullAccess 519
Utilização desta política 519
Detalhes desta política 519
Versão da política 519
Documento da política JSON 520
Saiba mais 523

AmazonDocDBElasticReadOnlyAccess 523
Utilização desta política 523
Detalhes desta política 523
Versão da política 523
Documento da política JSON 524
Saiba mais 524
AmazonDocDBFullAccess 525
Utilização desta política 525
Detalhes desta política 525
Versão da política 525
Documento da política JSON 525
Saiba mais 528
AmazonDocDBReadOnlyAccess 528
Utilização desta política 528
Detalhes desta política 528
Versão da política 529
Documento da política JSON 529
Saiba mais 531
AmazonDRSVPCManagement 531
Utilização desta política 531
Detalhes desta política 531
Versão da política 531
Documento da política JSON 531
Saiba mais 532
AmazonDynamoDBFullAccess 532
Utilização desta política 532
Detalhes desta política 533
Versão da política 533
Documento da política JSON 533
Saiba mais 536
AmazonDynamoDBFullAccess_v2 536
Utilização desta política 536
Detalhes desta política 536
Versão da política 536
Documento da política JSON 536
Saiba mais 540

AmazonDynamoDBFullAccesswithDataPipeline 540
Utilização desta política 540
Detalhes desta política 540
Versão da política 540
Documento da política JSON 541
Saiba mais 543
AmazonDynamoDBReadOnlyAccess 543
Utilização desta política 543
Detalhes desta política 543
Versão da política 543
Documento da política JSON 544
Saiba mais 545
AmazonEBSCSIDriverEKSClusterScopedPolicy 545
Utilização desta política 546
Detalhes desta política 546
Versão da política 546
Documento da política JSON 546
Saiba mais 551
AmazonEBSCSIDriverPolicy 551
Utilização desta política 552
Detalhes desta política 552
Versão da política 552
Documento da política JSON 552
Saiba mais 557
AmazonEBSCSIDriverPolicyV2 557
Utilização desta política 557
Detalhes desta política 557
Versão da política 557
Documento da política JSON 558
Saiba mais 562
AmazonEC2ContainerRegistryFullAccess 562
Utilização desta política 563
Detalhes desta política 563
Versão da política 563
Documento da política JSON 563
Saiba mais 564

AmazonEC2ContainerRegistryPowerUser 564
Utilização desta política 564
Detalhes desta política 564
Versão da política 565
Documento da política JSON 565
Saiba mais 565
AmazonEC2ContainerRegistryPullOnly 566
Utilização desta política 566
Detalhes desta política 566
Versão da política 566
Documento da política JSON 566
Saiba mais 567
AmazonEC2ContainerRegistryReadOnly 567
Utilização desta política 567
Detalhes desta política 567
Versão da política 567
Documento da política JSON 568
Saiba mais 568
AmazonEC2ContainerServiceAutoscaleRole 569
Utilização desta política 569
Detalhes desta política 569
Versão da política 569
Documento da política JSON 569
Saiba mais 570
AmazonEC2ContainerServiceEventsRole 570
Utilização desta política 570
Detalhes desta política 570
Versão da política 571
Documento da política JSON 571
Saiba mais 572
AmazonEC2ContainerServiceforEC2Role 572
Utilização desta política 572
Detalhes desta política 572
Versão da política 573
Documento da política JSON 573
Saiba mais 574

AmazonEC2ContainerServiceRole 574
Utilização desta política 574
Detalhes desta política 574
Versão da política 575
Documento da política JSON 575
Saiba mais 575
AmazonEC2FullAccess 576
Utilização desta política 576
Detalhes desta política 576
Versão da política 576
Documento da política JSON 576
Saiba mais 577
AmazonEC2ImageReferencesAccessPolicy 578
Utilização desta política 578
Detalhes desta política 578
Versão da política 578
Documento da política JSON 578
Saiba mais 579
AmazonEC2ReadOnlyAccess 579
Utilização desta política 579
Detalhes desta política 580
Versão da política 580
Documento da política JSON 580
Saiba mais 581
AmazonEC2RoleforAWSCodeDeploy 581
Utilização desta política 581
Detalhes desta política 581
Versão da política 581
Documento da política JSON 582
Saiba mais 582
AmazonEC2RoleforAWSCodeDeployLimited 582
Utilização desta política 582
Detalhes desta política 583
Versão da política 583
Documento da política JSON 583
Saiba mais 584

AmazonEC2RoleforDataPipelineRole 584
Utilização desta política 584
Detalhes desta política 584
Versão da política 584
Documento da política JSON 585
Saiba mais 585
AmazonEC2RoleforSSM 586
Utilização desta política 586
Detalhes desta política 586
Versão da política 586
Documento da política JSON 586
Saiba mais 589
AmazonEC2RolePolicyForLaunchWizard 589
Utilização desta política 589
Detalhes desta política 589
Versão da política 589
Documento da política JSON 589
Saiba mais 594
AmazonEC2SpotFleetAutoscaleRole 594
Utilização desta política 594
Detalhes desta política 594
Versão da política 595
Documento da política JSON 595
Saiba mais 596
AmazonEC2SpotFleetTaggingRole 596
Utilização desta política 596
Detalhes desta política 596
Versão da política 596
Documento da política JSON 597
Saiba mais 598
AmazonECS_FullAccess 598
Utilização desta política 598
Detalhes desta política 598
Versão da política 599
Documento da política JSON 599
Saiba mais 605

AmazonECSComputeServiceRolePolicy 605
Utilização desta política 605
Detalhes desta política 606
Versão da política 606
Documento da política JSON 606
Saiba mais 607
AmazonECSInfrastructureRoleforExpressGatewayServices 608
Utilização desta política 608
Detalhes desta política 608
Versão da política 608
Documento da política JSON 608
Saiba mais 615
AmazonECSInfrastructureRoleForGatewayHostSharedALB 615
Utilização desta política 615
Detalhes desta política 615
Versão da política 615
Documento da política JSON 616
Saiba mais 621
AmazonECSInfrastructureRolePolicyForLoadBalancers 621
Utilização desta política 621
Detalhes desta política 621
Versão da política 622
Documento da política JSON 622
Saiba mais 623
AmazonECSInfrastructureRolePolicyForManagedInstances 623
Utilização desta política 623
Detalhes desta política 624
Versão da política 624
Documento da política JSON 624
Saiba mais 629
AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity 629
Utilização desta política 629
Detalhes desta política 629
Versão da política 630
Documento da política JSON 630
Saiba mais 632

AmazonECSInfrastructureRolePolicyForVolumes 632
Utilização desta política 633
Detalhes desta política 633
Versão da política 633
Documento da política JSON 633
Saiba mais 635
AmazonECSInfrastructureRolePolicyForVpcLattice 636
Utilização desta política 636
Detalhes desta política 636
Versão da política 636
Documento da política JSON 636
Saiba mais 638
AmazonECSInstanceRolePolicyForManagedInstances 638
Utilização desta política 638
Detalhes desta política 638
Versão da política 639
Documento da política JSON 639
Saiba mais 640
AmazonECSServiceRolePolicy 640
Utilização desta política 641
Detalhes desta política 641
Versão da política 641
Documento da política JSON 641
Saiba mais 647
AmazonECSTaskExecutionRolePolicy 647
Utilização desta política 647
Detalhes desta política 647
Versão da política 647
Documento da política JSON 648
Saiba mais 648
AmazonEFSCSIDriverPolicy 648
Utilização desta política 648
Detalhes desta política 648
Versão da política 649
Documento da política JSON 649
Saiba mais 650

AmazonEKS_CNI_Policy 651
Utilização desta política 651
Detalhes desta política 651
Versão da política 651
Documento da política JSON 651
Saiba mais 652
AmazonEKSBlockStoragePolicy 652
Utilização desta política 653
Detalhes desta política 653
Versão da política 653
Documento da política JSON 653
Saiba mais 655
AmazonEKSBlockStoragePolicyV2 656
Utilização desta política 656
Detalhes desta política 656
Versão da política 656
Documento da política JSON 656
Saiba mais 659
AmazonEKSClusterPolicy 659
Utilização desta política 659
Detalhes desta política 659
Versão da política 659
Documento da política JSON 660
Saiba mais 662
AmazonEKSComputePolicy 662
Utilização desta política 662
Detalhes desta política 662
Versão da política 663
Documento da política JSON 663
Saiba mais 665
AmazonEKSConnectorServiceRolePolicy 666
Utilização desta política 666
Detalhes desta política 666
Versão da política 666
Documento da política JSON 666
Saiba mais 668

AmazonEKSDashboardConsoleReadOnly 668
Utilização desta política 669
Detalhes desta política 669
Versão da política 669
Documento da política JSON 669
Saiba mais 670
AmazonEKSDashboardServiceRolePolicy 670
Utilização desta política 671
Detalhes desta política 671
Versão da política 671
Documento da política JSON 671
Saiba mais 672
AmazonEKSFargatePodExecutionRolePolicy 672
Utilização desta política 672
Detalhes desta política 672
Versão da política 672
Documento da política JSON 673
Saiba mais 673
AmazonEKSForFargateServiceRolePolicy 673
Utilização desta política 673
Detalhes desta política 674
Versão da política 674
Documento da política JSON 674
Saiba mais 675
AmazonEKSLoadBalancingPolicy 675
Utilização desta política 675
Detalhes desta política 675
Versão da política 675
Documento da política JSON 675
Saiba mais 681
AmazonEKSLocalOutpostClusterPolicy 681
Utilização desta política 681
Detalhes desta política 681
Versão da política 682
Documento da política JSON 682
Saiba mais 684

AmazonEKSLocalOutpostServiceRolePolicy 684
Utilização desta política 684
Detalhes desta política 684
Versão da política 684
Documento da política JSON 685
Saiba mais 690
AmazonEKSMCPReadOnlyAccess 691
Utilização desta política 691
Detalhes desta política 691
Versão da política 691
Documento da política JSON 691
Saiba mais 693
AmazonEKSNetworkingPolicy 693
Utilização desta política 693
Detalhes desta política 694
Versão da política 694
Documento da política JSON 694
Saiba mais 696
AmazonEKSServicePolicy 696
Utilização desta política 696
Detalhes desta política 697
Versão da política 697
Documento da política JSON 697
Saiba mais 699
AmazonEKSServiceRolePolicy 699
Utilização desta política 699
Detalhes desta política 699
Versão da política 700
Documento da política JSON 700
Saiba mais 708
AmazonEKSVPCResourceController 708
Utilização desta política 708
Detalhes desta política 708
Versão da política 709
Documento da política JSON 709
Saiba mais 710

AmazonEKSWorkerNodeMinimalPolicy 710
Utilização desta política 710
Detalhes desta política 710
Versão da política 710
Documento da política JSON 711
Saiba mais 711
AmazonEKSWorkerNodePolicy 711
Utilização desta política 711
Detalhes desta política 711
Versão da política 712
Documento da política JSON 712
Saiba mais 712
AmazonElastiCacheFullAccess 713
Utilização desta política 713
Detalhes desta política 713
Versão da política 713
Documento da política JSON 713
Saiba mais 716
AmazonElastiCacheReadOnlyAccess 717
Utilização desta política 717
Detalhes desta política 717
Versão da política 717
Documento da política JSON 717
Saiba mais 718
AmazonElasticContainerRegistryPublicFullAccess 718
Utilização desta política 718
Detalhes desta política 718
Versão da política 718
Documento da política JSON 719
Saiba mais 719
AmazonElasticContainerRegistryPublicPowerUser 719
Utilização desta política 719
Detalhes desta política 720
Versão da política 720
Documento da política JSON 720
Saiba mais 721

AmazonElasticContainerRegistryPublicReadOnly 721
Utilização desta política 721
Detalhes desta política 721
Versão da política 721
Documento da política JSON 722
Saiba mais 722
AmazonElasticFileSystemClientFullAccess 722
Utilização desta política 723
Detalhes desta política 723
Versão da política 723
Documento da política JSON 723
Saiba mais 724
AmazonElasticFileSystemClientReadOnlyAccess 724
Utilização desta política 724
Detalhes desta política 724
Versão da política 724
Documento da política JSON 724
Saiba mais 725
AmazonElasticFileSystemClientReadWriteAccess 725
Utilização desta política 725
Detalhes desta política 725
Versão da política 726
Documento da política JSON 726
Saiba mais 726
AmazonElasticFileSystemFullAccess 726
Utilização desta política 727
Detalhes desta política 727
Versão da política 727
Documento da política JSON 727
Saiba mais 729
AmazonElasticFileSystemReadOnlyAccess 729
Utilização desta política 730
Detalhes desta política 730
Versão da política 730
Documento da política JSON 730
Saiba mais 731

AmazonElasticFileSystemServiceRolePolicy 731
Utilização desta política 731
Detalhes desta política 731
Versão da política 732
Documento da política JSON 732
Saiba mais 734
AmazonElasticFileSystemsUtils 734
Utilização desta política 734
Detalhes desta política 734
Versão da política 735
Documento da política JSON 735
Saiba mais 737
AmazonElasticMapReduceEditorsRole 737
Utilização desta política 737
Detalhes desta política 737
Versão da política 738
Documento da política JSON 738
Saiba mais 739
AmazonElasticMapReduceforAutoScalingRole 739
Utilização desta política 739
Detalhes desta política 739
Versão da política 740
Documento da política JSON 740
Saiba mais 740
AmazonElasticMapReduceforEC2Role 740
Utilização desta política 741
Detalhes desta política 741
Versão da política 741
Documento da política JSON 741
Saiba mais 742
AmazonElasticMapReduceFullAccess 743
Utilização desta política 743
Detalhes desta política 743
Versão da política 743
Documento da política JSON 743
Saiba mais 745

AmazonElasticMapReducePlacementGroupPolicy 746
Utilização desta política 746
Detalhes desta política 746
Versão da política 746
Documento da política JSON 746
Saiba mais 747
AmazonElasticMapReduceReadOnlyAccess 747
Utilização desta política 747
Detalhes desta política 747
Versão da política 748
Documento da política JSON 748
Saiba mais 748
AmazonElasticMapReduceRole 749
Utilização desta política 749
Detalhes desta política 749
Versão da política 749
Documento da política JSON 749
Saiba mais 751
AmazonElasticsearchServiceRolePolicy 752
Utilização desta política 752
Detalhes desta política 752
Versão da política 752
Documento da política JSON 752
Saiba mais 755
AmazonElasticTranscoder_FullAccess 755
Utilização desta política 756
Detalhes desta política 756
Versão da política 756
Documento da política JSON 756
Saiba mais 757
AmazonElasticTranscoder_JobsSubmitter 757
Utilização desta política 757
Detalhes desta política 757
Versão da política 758
Documento da política JSON 758
Saiba mais 758

AmazonElasticTranscoder_ReadOnlyAccess 759
Utilização desta política 759
Detalhes desta política 759
Versão da política 759
Documento da política JSON 759
Saiba mais 760
AmazonElasticTranscoderRole 760
Utilização desta política 760
Detalhes desta política 760
Versão da política 760
Documento da política JSON 761
Saiba mais 761
AmazonEMRCleanupPolicy 762
Utilização desta política 762
Detalhes desta política 762
Versão da política 762
Documento da política JSON 762
Saiba mais 763
AmazonEMRContainersServiceRolePolicy 763
Utilização desta política 763
Detalhes desta política 763
Versão da política 764
Documento da política JSON 764
Saiba mais 766
AmazonEMRFullAccessPolicy_v2 767
Utilização desta política 767
Detalhes desta política 767
Versão da política 767
Documento da política JSON 767
Saiba mais 771
AmazonEMRReadOnlyAccessPolicy_v2 771
Utilização desta política 771
Detalhes desta política 771
Versão da política 771
Documento da política JSON 772
Saiba mais 773

AmazonEMRServerlessServiceRolePolicy 773
Utilização desta política 773
Detalhes desta política 773
Versão da política 773
Documento da política JSON 774
Saiba mais 775
AmazonEMRServicePolicy_v2 775
Utilização desta política 775
Detalhes desta política 775
Versão da política 775
Documento da política JSON 775
Saiba mais 784
AmazonEMRServicePolicyForSessions 784
Utilização desta política 785
Detalhes desta política 785
Versão da política 785
Documento da política JSON 785
Saiba mais 789
AmazonESCognitoAccess 789
Utilização desta política 789
Detalhes desta política 789
Versão da política 789
Documento da política JSON 790
Saiba mais 790
AmazonESFullAccess 791
Utilização desta política 791
Detalhes desta política 791
Versão da política 791
Documento da política JSON 791
Saiba mais 792
AmazonESReadOnlyAccess 792
Utilização desta política 792
Detalhes desta política 792
Versão da política 792
Documento da política JSON 793
Saiba mais 793

AmazonEventBridgeApiDestinationsServiceRolePolicy 793
Utilização desta política 793
Detalhes desta política 794
Versão da política 794
Documento da política JSON 794
Saiba mais 795
AmazonEventBridgeFullAccess 795
Utilização desta política 795
Detalhes desta política 795
Versão da política 796
Documento da política JSON 796
Saiba mais 798
AmazonEventBridgePipesFullAccess 798
Utilização desta política 798
Detalhes desta política 798
Versão da política 799
Documento da política JSON 799
Saiba mais 799
AmazonEventBridgePipesOperatorAccess 800
Utilização desta política 800
Detalhes desta política 800
Versão da política 800
Documento da política JSON 800
Saiba mais 801
AmazonEventBridgePipesReadOnlyAccess 801
Utilização desta política 801
Detalhes desta política 801
Versão da política 801
Documento da política JSON 802
Saiba mais 802
AmazonEventBridgeReadOnlyAccess 802
Utilização desta política 802
Detalhes desta política 802
Versão da política 803
Documento da política JSON 803
Saiba mais 804

AmazonEventBridgeSchedulerFullAccess 804
Utilização desta política 805
Detalhes desta política 805
Versão da política 805
Documento da política JSON 805
Saiba mais 806
AmazonEventBridgeSchedulerReadOnlyAccess 806
Utilização desta política 806
Detalhes desta política 806
Versão da política 806
Documento da política JSON 807
Saiba mais 807
AmazonEventBridgeSchemasFullAccess 807
Utilização desta política 807
Detalhes desta política 808
Versão da política 808
Documento da política JSON 808
Saiba mais 809
AmazonEventBridgeSchemasReadOnlyAccess 809
Utilização desta política 809
Detalhes desta política 809
Versão da política 810
Documento da política JSON 810
Saiba mais 810
AmazonEventBridgeSchemasServiceRolePolicy 811
Utilização desta política 811
Detalhes desta política 811
Versão da política 811
Documento da política JSON 811
Saiba mais 812
AmazonEVSServiceRolePolicy 812
Utilização desta política 812
Detalhes desta política 812
Versão da política 813
Documento da política JSON 813
Saiba mais 818

AmazonFISServiceRolePolicy 818
Utilização desta política 818
Detalhes desta política 818
Versão da política 819
Documento da política JSON 819
Saiba mais 820
AmazonForecastFullAccess 821
Utilização desta política 821
Detalhes desta política 821
Versão da política 821
Documento da política JSON 821
Saiba mais 822
AmazonFraudDetectorFullAccessPolicy 822
Utilização desta política 822
Detalhes desta política 822
Versão da política 823
Documento da política JSON 823
Saiba mais 824
AmazonFreeRTOSFullAccess 824
Utilização desta política 824
Detalhes desta política 824
Versão da política 825
Documento da política JSON 825
Saiba mais 825
AmazonFreeRTOSOTAUpdate 825
Utilização desta política 825
Detalhes desta política 826
Versão da política 826
Documento da política JSON 826
Saiba mais 827
AmazonFSxConsoleFullAccess 828
Utilização desta política 828
Detalhes desta política 828
Versão da política 828
Documento da política JSON 828
Saiba mais 832

AmazonFSxConsoleReadOnlyAccess 832
Utilização desta política 832
Detalhes desta política 832
Versão da política 832
Documento da política JSON 833
Saiba mais 833
AmazonFSxFullAccess 833
Utilização desta política 834
Detalhes desta política 834
Versão da política 834
Documento da política JSON 834
Saiba mais 838
AmazonFSxReadOnlyAccess 838
Utilização desta política 839
Detalhes desta política 839
Versão da política 839
Documento da política JSON 839
Saiba mais 839
AmazonFSxServiceRolePolicy 840
Utilização desta política 840
Detalhes desta política 840
Versão da política 840
Documento da política JSON 840
Saiba mais 843
AmazonGlacierFullAccess 843
Utilização desta política 843
Detalhes desta política 844
Versão da política 844
Documento da política JSON 844
Saiba mais 844
AmazonGlacierReadOnlyAccess 845
Utilização desta política 845
Detalhes desta política 845
Versão da política 845
Documento da política JSON 845
Saiba mais 846

AmazonGrafanaAthenaAccess 846
Utilização desta política 846
Detalhes desta política 846
Versão da política 847
Documento da política JSON 847
Saiba mais 848
AmazonGrafanaCloudWatchAccess 849
Utilização desta política 849
Detalhes desta política 849
Versão da política 849
Documento da política JSON 849
Saiba mais 851
AmazonGrafanaRedshiftAccess 851
Utilização desta política 851
Detalhes desta política 851
Versão da política 851
Documento da política JSON 852
Saiba mais 853
AmazonGrafanaServiceLinkedRolePolicy 853
Utilização desta política 853
Detalhes desta política 853
Versão da política 854
Documento da política JSON 854
Saiba mais 855
AmazonGuardDutyFullAccess 855
Utilização desta política 855
Detalhes desta política 855
Versão da política 856
Documento da política JSON 856
Saiba mais 857
AmazonGuardDutyFullAccess_v2 857
Utilização desta política 858
Detalhes desta política 858
Versão da política 858
Documento da política JSON 858
Saiba mais 860

AmazonGuardDutyMalwareProtectionServiceRolePolicy 860
Utilização desta política 861
Detalhes desta política 861
Versão da política 861
Documento da política JSON 861
Saiba mais 866
AmazonGuardDutyReadOnlyAccess 866
Utilização desta política 866
Detalhes desta política 866
Versão da política 866
Documento da política JSON 866
Saiba mais 867
AmazonGuardDutyServiceRolePolicy 867
Utilização desta política 868
Detalhes desta política 868
Versão da política 868
Documento da política JSON 868
Saiba mais 875
AmazonHealthLakeFullAccess 875
Utilização desta política 875
Detalhes desta política 875
Versão da política 875
Documento da política JSON 876
Saiba mais 876
AmazonHealthLakeReadOnlyAccess 877
Utilização desta política 877
Detalhes desta política 877
Versão da política 877
Documento da política JSON 877
Saiba mais 878
AmazonHoneycodeFullAccess 878
Utilização desta política 878
Detalhes desta política 878
Versão da política 879
Documento da política JSON 879
Saiba mais 879

AmazonHoneycodeReadOnlyAccess 879
Utilização desta política 880
Detalhes desta política 880
Versão da política 880
Documento da política JSON 880
Saiba mais 881
AmazonHoneycodeServiceRolePolicy 881
Utilização desta política 881
Detalhes desta política 881
Versão da política 881
Documento da política JSON 882
Saiba mais 882
AmazonHoneycodeTeamAssociationFullAccess 882
Utilização desta política 882
Detalhes desta política 882
Versão da política 883
Documento da política JSON 883
Saiba mais 883
AmazonHoneycodeTeamAssociationReadOnlyAccess 883
Utilização desta política 884
Detalhes desta política 884
Versão da política 884
Documento da política JSON 884
Saiba mais 884
AmazonHoneycodeWorkbookFullAccess 885
Utilização desta política 885
Detalhes desta política 885
Versão da política 885
Documento da política JSON 885
Saiba mais 886
AmazonHoneycodeWorkbookReadOnlyAccess 886
Utilização desta política 886
Detalhes desta política 886
Versão da política 887
Documento da política JSON 887
Saiba mais 887

AmazonInspector2AgentlessServiceRolePolicy 888
Utilização desta política 888
Detalhes desta política 888
Versão da política 888
Documento da política JSON 888
Saiba mais 893
AmazonInspector2AmiScanServiceRolePolicy 893
Utilização desta política 893
Detalhes desta política 893
Versão da política 894
Documento da política JSON 894
Saiba mais 897
AmazonInspector2FullAccess 897
Utilização desta política 898
Detalhes desta política 898
Versão da política 898
Documento da política JSON 898
Saiba mais 899
AmazonInspector2FullAccess_v2 900
Utilização desta política 900
Detalhes desta política 900
Versão da política 900
Documento da política JSON 900
Saiba mais 903
AmazonInspector2ManagedCisPolicy 904
Utilização desta política 904
Detalhes desta política 904
Versão da política 904
Documento da política JSON 904
Saiba mais 905
AmazonInspector2ManagedTelemetryPolicy 905
Utilização desta política 905
Detalhes desta política 905
Versão da política 905
Documento da política JSON 906
Saiba mais 906

AmazonInspector2ReadOnlyAccess 906
Utilização desta política 907
Detalhes desta política 907
Versão da política 907
Documento da política JSON 907
Saiba mais 909
AmazonInspector2ServiceRolePolicy 909
Utilização desta política 909
Detalhes desta política 909
Versão da política 910
Documento da política JSON 910
Saiba mais 918
AmazonInspector2ThirdPartyServiceRolePolicy 918
Utilização desta política 918
Detalhes desta política 918
Versão da política 919
Documento da política JSON 919
Saiba mais 923
AmazonInspectorFullAccess 923
Utilização desta política 924
Detalhes desta política 924
Versão da política 924
Documento da política JSON 924
Saiba mais 925
AmazonInspectorReadOnlyAccess 925
Utilização desta política 925
Detalhes desta política 926
Versão da política 926
Documento da política JSON 926
Saiba mais 927
AmazonInspectorServiceRolePolicy 927
Utilização desta política 927
Detalhes desta política 927
Versão da política 927
Documento da política JSON 928
Saiba mais 929

AmazonKendraFullAccess 929
Utilização desta política 929
Detalhes desta política 929
Versão da política 929
Documento da política JSON 930
Saiba mais 931
AmazonKendraReadOnlyAccess 932
Utilização desta política 932
Detalhes desta política 932
Versão da política 932
Documento da política JSON 932
Saiba mais 933
AmazonKeyspacesFullAccess 933
Utilização desta política 933
Detalhes desta política 933
Versão da política 933
Documento da política JSON 934
Saiba mais 936
AmazonKeyspacesReadOnlyAccess 936
Utilização desta política 936
Detalhes desta política 936
Versão da política 936
Documento da política JSON 937
Saiba mais 937
AmazonKeyspacesReadOnlyAccess_v2 938
Utilização desta política 938
Detalhes desta política 938
Versão da política 938
Documento da política JSON 938
Saiba mais 939
AmazonKinesisAnalyticsFullAccess 940
Utilização desta política 940
Detalhes desta política 940
Versão da política 940
Documento da política JSON 940
Saiba mais 942

AmazonKinesisAnalyticsReadOnly 942
Utilização desta política 942
Detalhes desta política 942
Versão da política 942
Documento da política JSON 943
Saiba mais 944
AmazonKinesisFirehoseFullAccess 944
Utilização desta política 944
Detalhes desta política 944
Versão da política 944
Documento da política JSON 945
Saiba mais 945
AmazonKinesisFirehoseReadOnlyAccess 945
Utilização desta política 945
Detalhes desta política 946
Versão da política 946
Documento da política JSON 946
Saiba mais 946
AmazonKinesisFullAccess 947
Utilização desta política 947
Detalhes desta política 947
Versão da política 947
Documento da política JSON 947
Saiba mais 948
AmazonKinesisReadOnlyAccess 948
Utilização desta política 948
Detalhes desta política 948
Versão da política 948
Documento da política JSON 948
Saiba mais 949
AmazonKinesisVideoStreamsFullAccess 949
Utilização desta política 949
Detalhes desta política 949
Versão da política 950
Documento da política JSON 950
Saiba mais 950

AmazonKinesisVideoStreamsReadOnlyAccess 950
Utilização desta política 950
Detalhes desta política 951
Versão da política 951
Documento da política JSON 951
Saiba mais 951
AmazonLaunchWizard_Fullaccess 952
Utilização desta política 952
Detalhes desta política 952
Versão da política 952
Documento da política JSON 952
Saiba mais 966
AmazonLaunchWizardFullAccessV2 967
Utilização desta política 967
Detalhes desta política 967
Versão da política 967
Documento da política JSON 967
Saiba mais 989
AmazonLexChannelsAccess 989
Utilização desta política 989
Detalhes desta política 989
Versão da política 989
Documento da política JSON 990
Saiba mais 990
AmazonLexFullAccess 990
Utilização desta política 990
Detalhes desta política 990
Versão da política 991
Documento da política JSON 991
Saiba mais 996
AmazonLexReadOnly 997
Utilização desta política 997
Detalhes desta política 997
Versão da política 997
Documento da política JSON 997
Saiba mais 999

AmazonLexReplicationPolicy 999
Utilização desta política 999
Detalhes desta política 999
Versão da política 999
Documento da política JSON 1000
Saiba mais 1002
AmazonLexRunBotsOnly 1002
Utilização desta política 1002
Detalhes desta política 1002
Versão da política 1003
Documento da política JSON 1003
Saiba mais 1003
AmazonLexV2BotPolicy 1003
Utilização desta política 1004
Detalhes desta política 1004
Versão da política 1004
Documento da política JSON 1004
Saiba mais 1005
AmazonLookoutEquipmentFullAccess 1005
Utilização desta política 1005
Detalhes desta política 1005
Versão da política 1005
Documento da política JSON 1005
Saiba mais 1007
AmazonLookoutEquipmentReadOnlyAccess 1007
Utilização desta política 1007
Detalhes desta política 1007
Versão da política 1007
Documento da política JSON 1007
Saiba mais 1008
AmazonLookoutMetricsFullAccess 1008
Utilização desta política 1008
Detalhes desta política 1008
Versão da política 1009
Documento da política JSON 1009
Saiba mais 1009

AmazonLookoutMetricsReadOnlyAccess 1010
Utilização desta política 1010
Detalhes desta política 1010
Versão da política 1010
Documento da política JSON 1010
Saiba mais 1011
AmazonLookoutVisionConsoleFullAccess 1011
Utilização desta política 1011
Detalhes desta política 1011
Versão da política 1012
Documento da política JSON 1012
Saiba mais 1014
AmazonLookoutVisionConsoleReadOnlyAccess 1014
Utilização desta política 1014
Detalhes desta política 1014
Versão da política 1015
Documento da política JSON 1015
Saiba mais 1016
AmazonLookoutVisionFullAccess 1016
Utilização desta política 1016
Detalhes desta política 1017
Versão da política 1017
Documento da política JSON 1017
Saiba mais 1017
AmazonLookoutVisionReadOnlyAccess 1018
Utilização desta política 1018
Detalhes desta política 1018
Versão da política 1018
Documento da política JSON 1018
Saiba mais 1019
AmazonMachineLearningBatchPredictionsAccess 1019
Utilização desta política 1019
Detalhes desta política 1019
Versão da política 1020
Documento da política JSON 1020
Saiba mais 1020

AmazonMachineLearningCreateOnlyAccess 1020
Utilização desta política 1021
Detalhes desta política 1021
Versão da política 1021
Documento da política JSON 1021
Saiba mais 1022
AmazonMachineLearningFullAccess 1022
Utilização desta política 1022
Detalhes desta política 1022
Versão da política 1022
Documento da política JSON 1022
Saiba mais 1023
AmazonMachineLearningManageRealTimeEndpointOnlyAccess 1023
Utilização desta política 1023
Detalhes desta política 1023
Versão da política 1024
Documento da política JSON 1024
Saiba mais 1024
AmazonMachineLearningReadOnlyAccess 1024
Utilização desta política 1025
Detalhes desta política 1025
Versão da política 1025
Documento da política JSON 1025
Saiba mais 1025
AmazonMachineLearningRealTimePredictionOnlyAccess 1026
Utilização desta política 1026
Detalhes desta política 1026
Versão da política 1026
Documento da política JSON 1026
Saiba mais 1027
AmazonMachineLearningRoleforRedshiftDataSourceV3 1027
Utilização desta política 1027
Detalhes desta política 1027
Versão da política 1028
Documento da política JSON 1028
Saiba mais 1029

AmazonMacieFullAccess 1029
Utilização desta política 1029
Detalhes desta política 1029
Versão da política 1029
Documento da política JSON 1030
Saiba mais 1030
AmazonMacieHandshakeRole 1031
Utilização desta política 1031
Detalhes desta política 1031
Versão da política 1031
Documento da política JSON 1031
Saiba mais 1032
AmazonMacieReadOnlyAccess 1032
Utilização desta política 1032
Detalhes desta política 1032
Versão da política 1032
Documento da política JSON 1033
Saiba mais 1033
AmazonMacieServiceRole 1033
Utilização desta política 1033
Detalhes desta política 1034
Versão da política 1034
Documento da política JSON 1034
Saiba mais 1034
AmazonMacieServiceRolePolicy 1035
Utilização desta política 1035
Detalhes desta política 1035
Versão da política 1035
Documento da política JSON 1035
Saiba mais 1037
AmazonManagedBlockchainConsoleFullAccess 1037
Utilização desta política 1037
Detalhes desta política 1037
Versão da política 1037
Documento da política JSON 1037
Saiba mais 1038

AmazonManagedBlockchainFullAccess 1038
Utilização desta política 1038
Detalhes desta política 1038
Versão da política 1039
Documento da política JSON 1039
Saiba mais 1039
AmazonManagedBlockchainReadOnlyAccess 1039
Utilização desta política 1040
Detalhes desta política 1040
Versão da política 1040
Documento da política JSON 1040
Saiba mais 1041
AmazonManagedBlockchainServiceRolePolicy 1041
Utilização desta política 1041
Detalhes desta política 1041
Versão da política 1041
Documento da política JSON 1042
Saiba mais 1042
AmazonMCSFullAccess 1042
Utilização desta política 1042
Detalhes desta política 1043
Versão da política 1043
Documento da política JSON 1043
Saiba mais 1044
AmazonMCSReadOnlyAccess 1044
Utilização desta política 1045
Detalhes desta política 1045
Versão da política 1045
Documento da política JSON 1045
Saiba mais 1046
AmazonMechanicalTurkFullAccess 1046
Utilização desta política 1046
Detalhes desta política 1046
Versão da política 1046
Documento da política JSON 1047
Saiba mais 1047

AmazonMechanicalTurkReadOnly 1047
Utilização desta política 1047
Detalhes desta política 1047
Versão da política 1048
Documento da política JSON 1048
Saiba mais 1048
AmazonMemoryDBFullAccess 1049
Utilização desta política 1049
Detalhes desta política 1049
Versão da política 1049
Documento da política JSON 1049
Saiba mais 1050
AmazonMemoryDBReadOnlyAccess 1050
Utilização desta política 1050
Detalhes desta política 1050
Versão da política 1051
Documento da política JSON 1051
Saiba mais 1051
AmazonMobileAnalyticsFinancialReportAccess 1051
Utilização desta política 1052
Detalhes desta política 1052
Versão da política 1052
Documento da política JSON 1052
Saiba mais 1052
AmazonMobileAnalyticsFullAccess 1053
Utilização desta política 1053
Detalhes desta política 1053
Versão da política 1053
Documento da política JSON 1053
Saiba mais 1054
AmazonMobileAnalyticsNon-financialReportAccess 1054
Utilização desta política 1054
Detalhes desta política 1054
Versão da política 1054
Documento da política JSON 1055
Saiba mais 1055

AmazonMobileAnalyticsWriteOnlyAccess 1055
Utilização desta política 1055
Detalhes desta política 1055
Versão da política 1056
Documento da política JSON 1056
Saiba mais 1056
AmazonMonitronFullAccess 1056
Utilização desta política 1057
Detalhes desta política 1057
Versão da política 1057
Documento da política JSON 1057
Saiba mais 1059
AmazonMQApiFullAccess 1059
Utilização desta política 1059
Detalhes desta política 1059
Versão da política 1060
Documento da política JSON 1060
Saiba mais 1061
AmazonMQApiReadOnlyAccess 1061
Utilização desta política 1061
Detalhes desta política 1061
Versão da política 1061
Documento da política JSON 1062
Saiba mais 1062
AmazonMQFullAccess 1062
Utilização desta política 1062
Detalhes desta política 1063
Versão da política 1063
Documento da política JSON 1063
Saiba mais 1065
AmazonMQReadOnlyAccess 1065
Utilização desta política 1065
Detalhes desta política 1065
Versão da política 1065
Documento da política JSON 1065
Saiba mais 1066

AmazonMQServiceRolePolicy 1066
Utilização desta política 1066
Detalhes desta política 1066
Versão da política 1067
Documento da política JSON 1067
Saiba mais 1069
AmazonMSKConnectReadOnlyAccess 1069
Utilização desta política 1069
Detalhes desta política 1069
Versão da política 1069
Documento da política JSON 1069
Saiba mais 1070
AmazonMSKFullAccess 1071
Utilização desta política 1071
Detalhes desta política 1071
Versão da política 1071
Documento da política JSON 1071
Saiba mais 1074
AmazonMSKReadOnlyAccess 1074
Utilização desta política 1074
Detalhes desta política 1075
Versão da política 1075
Documento da política JSON 1075
Saiba mais 1075
AmazonMWAAServerlessServiceRolePolicy 1076
Utilização desta política 1076
Detalhes desta política 1076
Versão da política 1076
Documento da política JSON 1076
Saiba mais 1077
AmazonMWAAServiceRolePolicy 1077
Utilização desta política 1077
Detalhes desta política 1077
Versão da política 1078
Documento da política JSON 1078
Saiba mais 1080

AmazonNimbleStudio-LaunchProfileWorker 1080
Utilização desta política 1080
Detalhes desta política 1081
Versão da política 1081
Documento da política JSON 1081
Saiba mais 1082
AmazonNimbleStudio-StudioAdmin 1082
Utilização desta política 1082
Detalhes desta política 1082
Versão da política 1082
Documento da política JSON 1082
Saiba mais 1084
AmazonNimbleStudio-StudioUser 1085
Utilização desta política 1085
Detalhes desta política 1085
Versão da política 1085
Documento da política JSON 1085
Saiba mais 1087
AmazonODBAutonomousDatabaseAdmin 1088
Utilização desta política 1088
Detalhes desta política 1088
Versão da política 1088
Documento da política JSON 1088
Saiba mais 1090
AmazonODBAutonomousVmClusterAdmin 1091
Utilização desta política 1091
Detalhes desta política 1091
Versão da política 1091
Documento da política JSON 1091
Saiba mais 1093
AmazonODBExadataInfrastructureAdmin 1093
Utilização desta política 1093
Detalhes desta política 1093
Versão da política 1094
Documento da política JSON 1094
Saiba mais 1095

AmazonODBExadataVmClusterAdmin 1096
Utilização desta política 1096
Detalhes desta política 1096
Versão da política 1096
Documento da política JSON 1096
Saiba mais 1098
AmazonODBExascaleStorageVaultAdmin 1098
Utilização desta política 1098
Detalhes desta política 1098
Versão da política 1099
Documento da política JSON 1099
Saiba mais 1100
AmazonODBExascaleVmClusterAdmin 1101
Utilização desta política 1101
Detalhes desta política 1101
Versão da política 1101
Documento da política JSON 1101
Saiba mais 1103
AmazonODBFullAccess 1103
Utilização desta política 1103
Detalhes desta política 1103
Versão da política 1104
Documento da política JSON 1104
Saiba mais 1107
AmazonODBNetworkAdmin 1107
Utilização desta política 1107
Detalhes desta política 1107
Versão da política 1108
Documento da política JSON 1108
Saiba mais 1110
AmazonODBReadOnlyAccess 1110
Utilização desta política 1110
Detalhes desta política 1110
Versão da política 1110
Documento da política JSON 1111
Saiba mais 1112

AmazonODBServiceRolePolicy 1112
Utilização desta política 1112
Detalhes desta política 1112
Versão da política 1113
Documento da política JSON 1113
Saiba mais 1114
AmazonOmicsFullAccess 1114
Utilização desta política 1115
Detalhes desta política 1115
Versão da política 1115
Documento da política JSON 1115
Saiba mais 1116
AmazonOmicsReadOnlyAccess 1116
Utilização desta política 1116
Detalhes desta política 1116
Versão da política 1117
Documento da política JSON 1117
Saiba mais 1117
AmazonOneEnterpriseFullAccess 1117
Utilização desta política 1118
Detalhes desta política 1118
Versão da política 1118
Documento da política JSON 1118
Saiba mais 1118
AmazonOneEnterpriseInstallerAccess 1119
Utilização desta política 1119
Detalhes desta política 1119
Versão da política 1119
Documento da política JSON 1119
Saiba mais 1120
AmazonOneEnterpriseReadOnlyAccess 1120
Utilização desta política 1120
Detalhes desta política 1120
Versão da política 1121
Documento da política JSON 1121
Saiba mais 1121

AmazonOpenSearchDashboardsServiceRolePolicy 1121
Utilização desta política 1122
Detalhes desta política 1122
Versão da política 1122
Documento da política JSON 1122
Saiba mais 1123
AmazonOpenSearchDirectQueryGlueCreateAccess 1123
Utilização desta política 1123
Detalhes desta política 1123
Versão da política 1123
Documento da política JSON 1123
Saiba mais 1124
AmazonOpenSearchIngestionFullAccess 1124
Utilização desta política 1124
Detalhes desta política 1124
Versão da política 1125
Documento da política JSON 1125
Saiba mais 1126
AmazonOpenSearchIngestionReadOnlyAccess 1126
Utilização desta política 1126
Detalhes desta política 1126
Versão da política 1126
Documento da política JSON 1127
Saiba mais 1127
AmazonOpenSearchIngestionServiceRolePolicy 1127
Utilização desta política 1127
Detalhes desta política 1128
Versão da política 1128
Documento da política JSON 1128
Saiba mais 1130
AmazonOpenSearchServerlessServiceRolePolicy 1130
Utilização desta política 1130
Detalhes desta política 1130
Versão da política 1131
Documento da política JSON 1131
Saiba mais 1131

AmazonOpenSearchServiceCognitoAccess 1131
Utilização desta política 1132
Detalhes desta política 1132
Versão da política 1132
Documento da política JSON 1132
Saiba mais 1133
AmazonOpenSearchServiceFullAccess 1133
Utilização desta política 1134
Detalhes desta política 1134
Versão da política 1134
Documento da política JSON 1134
Saiba mais 1134
AmazonOpenSearchServiceReadOnlyAccess 1135
Utilização desta política 1135
Detalhes desta política 1135
Versão da política 1135
Documento da política JSON 1135
Saiba mais 1136
AmazonOpenSearchServiceRolePolicy 1136
Utilização desta política 1136
Detalhes desta política 1136
Versão da política 1137
Documento da política JSON 1137
Saiba mais 1142
AmazonPersonalizeFullAccess 1142
Utilização desta política 1142
Detalhes desta política 1142
Versão da política 1142
Documento da política JSON 1142
Saiba mais 1144
AmazonPollyFullAccess 1144
Utilização desta política 1144
Detalhes desta política 1144
Versão da política 1144
Documento da política JSON 1144
Saiba mais 1145

AmazonPollyReadOnlyAccess 1145
Utilização desta política 1145
Detalhes desta política 1145
Versão da política 1145
Documento da política JSON 1146
Saiba mais 1146
AmazonPrometheusConsoleFullAccess 1146
Utilização desta política 1147
Detalhes desta política 1147
Versão da política 1147
Documento da política JSON 1147
Saiba mais 1148
AmazonPrometheusFullAccess 1148
Utilização desta política 1149
Detalhes desta política 1149
Versão da política 1149
Documento da política JSON 1149
Saiba mais 1150
AmazonPrometheusQueryAccess 1150
Utilização desta política 1150
Detalhes desta política 1151
Versão da política 1151
Documento da política JSON 1151
Saiba mais 1151
AmazonPrometheusRemoteWriteAccess 1152
Utilização desta política 1152
Detalhes desta política 1152
Versão da política 1152
Documento da política JSON 1152
Saiba mais 1153
AmazonPrometheusScraperServiceRolePolicy 1153
Utilização desta política 1153
Detalhes desta política 1153
Versão da política 1153
Documento da política JSON 1154
Saiba mais 1156

AmazonQDeveloperAccess 1156
Utilização desta política 1157
Detalhes desta política 1157
Versão da política 1157
Documento da política JSON 1157
Saiba mais 1158
AmazonQFullAccess 1159
Utilização desta política 1159
Detalhes desta política 1159
Versão da política 1159
Documento da política JSON 1159
Saiba mais 1161
AmazonQLDBConsoleFullAccess 1161
Utilização desta política 1161
Detalhes desta política 1162
Versão da política 1162
Documento da política JSON 1162
Saiba mais 1164
AmazonQLDBFullAccess 1164
Utilização desta política 1164
Detalhes desta política 1164
Versão da política 1164
Documento da política JSON 1165
Saiba mais 1166
AmazonQLDBReadOnly 1166
Utilização desta política 1166
Detalhes desta política 1166
Versão da política 1167
Documento da política JSON 1167
Saiba mais 1167
AmazonRDSBetaServiceRolePolicy 1168
Utilização desta política 1168
Detalhes desta política 1168
Versão da política 1168
Documento da política JSON 1168
Saiba mais 1171

AmazonRDSCustomInstanceProfileRolePolicy 1171
Utilização desta política 1172
Detalhes desta política 1172
Versão da política 1172
Documento da política JSON 1172
Saiba mais 1179
AmazonRDSCustomPreviewServiceRolePolicy 1179
Utilização desta política 1180
Detalhes desta política 1180
Versão da política 1180
Documento da política JSON 1180
Saiba mais 1198
AmazonRDSCustomServiceRolePolicy 1198
Utilização desta política 1198
Detalhes desta política 1198
Versão da política 1198
Documento da política JSON 1199
Saiba mais 1217
AmazonRDSDataFullAccess 1218
Utilização desta política 1218
Detalhes desta política 1218
Versão da política 1218
Documento da política JSON 1218
Saiba mais 1219
AmazonRDSDirectoryServiceAccess 1220
Utilização desta política 1220
Detalhes desta política 1220
Versão da política 1220
Documento da política JSON 1220
Saiba mais 1221
AmazonRDSEnhancedMonitoringRole 1221
Utilização desta política 1221
Detalhes desta política 1221
Versão da política 1221
Documento da política JSON 1222
Saiba mais 1222

AmazonRDSFullAccess 1223
Utilização desta política 1223
Detalhes desta política 1223
Versão da política 1223
Documento da política JSON 1223
Saiba mais 1225
AmazonRDSPerformanceInsightsFullAccess 1225
Utilização desta política 1226
Detalhes desta política 1226
Versão da política 1226
Documento da política JSON 1226
Saiba mais 1228
AmazonRDSPerformanceInsightsReadOnly 1228
Utilização desta política 1228
Detalhes desta política 1228
Versão da política 1228
Documento da política JSON 1229
Saiba mais 1231
AmazonRDSPreviewServiceRolePolicy 1231
Utilização desta política 1231
Detalhes desta política 1231
Versão da política 1232
Documento da política JSON 1232
Saiba mais 1235
AmazonRDSReadOnlyAccess 1235
Utilização desta política 1235
Detalhes desta política 1235
Versão da política 1235
Documento da política JSON 1236
Saiba mais 1237
AmazonRDSServiceRolePolicy 1237
Utilização desta política 1237
Detalhes desta política 1237
Versão da política 1238
Documento da política JSON 1238
Saiba mais 1241

AmazonRedshiftAllCommandsFullAccess 1242
Utilização desta política 1242
Detalhes desta política 1242
Versão da política 1242
Documento da política JSON 1242
Saiba mais 1248
AmazonRedshiftDataFullAccess 1248
Utilização desta política 1248
Detalhes desta política 1248
Versão da política 1248
Documento da política JSON 1248
Saiba mais 1250
AmazonRedshiftFederatedAuthorization 1251
Utilização desta política 1251
Detalhes desta política 1251
Versão da política 1251
Documento da política JSON 1251
Saiba mais 1252
AmazonRedshiftFullAccess 1253
Utilização desta política 1253
Detalhes desta política 1253
Versão da política 1253
Documento da política JSON 1253
Saiba mais 1255
AmazonRedshiftQueryEditor 1255
Utilização desta política 1256
Detalhes desta política 1256
Versão da política 1256
Documento da política JSON 1256
Saiba mais 1258
AmazonRedshiftQueryEditorV2FullAccess 1258
Utilização desta política 1258
Detalhes desta política 1259
Versão da política 1259
Documento da política JSON 1259
Saiba mais 1260

AmazonRedshiftQueryEditorV2NoSharing 1261
Utilização desta política 1261
Detalhes desta política 1261
Versão da política 1261
Documento da política JSON 1261
Saiba mais 1265
AmazonRedshiftQueryEditorV2ReadSharing 1265
Utilização desta política 1265
Detalhes desta política 1266
Versão da política 1266
Documento da política JSON 1266
Saiba mais 1271
AmazonRedshiftQueryEditorV2ReadWriteSharing 1271
Utilização desta política 1271
Detalhes desta política 1271
Versão da política 1272
Documento da política JSON 1272
Saiba mais 1277
AmazonRedshiftReadOnlyAccess 1277
Utilização desta política 1277
Detalhes desta política 1277
Versão da política 1277
Documento da política JSON 1278
Saiba mais 1278
AmazonRedshiftServiceLinkedRolePolicy 1279
Utilização desta política 1279
Detalhes desta política 1279
Versão da política 1279
Documento da política JSON 1279
Saiba mais 1286
AmazonRekognitionCustomLabelsFullAccess 1286
Utilização desta política 1286
Detalhes desta política 1286
Versão da política 1286
Documento da política JSON 1286
Saiba mais 1288

AmazonRekognitionFullAccess 1288
Utilização desta política 1288
Detalhes desta política 1288
Versão da política 1288
Documento da política JSON 1288
Saiba mais 1289
AmazonRekognitionReadOnlyAccess 1289
Utilização desta política 1289
Detalhes desta política 1289
Versão da política 1290
Documento da política JSON 1290
Saiba mais 1291
AmazonRekognitionServiceRole 1291
Utilização desta política 1291
Detalhes desta política 1291
Versão da política 1292
Documento da política JSON 1292
Saiba mais 1292
AmazonRoute53AutoNamingFullAccess 1293
Utilização desta política 1293
Detalhes desta política 1293
Versão da política 1293
Documento da política JSON 1293
Saiba mais 1294
AmazonRoute53AutoNamingReadOnlyAccess 1294
Utilização desta política 1294
Detalhes desta política 1295
Versão da política 1295
Documento da política JSON 1295
Saiba mais 1295
AmazonRoute53AutoNamingRegistrantAccess 1296
Utilização desta política 1296
Detalhes desta política 1296
Versão da política 1296
Documento da política JSON 1296
Saiba mais 1297

AmazonRoute53DomainsFullAccess 1297
Utilização desta política 1297
Detalhes desta política 1297
Versão da política 1298
Documento da política JSON 1298
Saiba mais 1298
AmazonRoute53DomainsReadOnlyAccess 1299
Utilização desta política 1299
Detalhes desta política 1299
Versão da política 1299
Documento da política JSON 1299
Saiba mais 1300
AmazonRoute53FullAccess 1300
Utilização desta política 1300
Detalhes desta política 1300
Versão da política 1300
Documento da política JSON 1301
Saiba mais 1302
AmazonRoute53GlobalResolverFullAccess 1302
Utilização desta política 1302
Detalhes desta política 1302
Versão da política 1302
Documento da política JSON 1302
Saiba mais 1304
AmazonRoute53GlobalResolverReadOnlyAccess 1304
Utilização desta política 1304
Detalhes desta política 1305
Versão da política 1305
Documento da política JSON 1305
Saiba mais 1306
AmazonRoute53ProfilesFullAccess 1306
Utilização desta política 1306
Detalhes desta política 1306
Versão da política 1306
Documento da política JSON 1307
Saiba mais 1308

AmazonRoute53ProfilesReadOnlyAccess 1308
Utilização desta política 1308
Detalhes desta política 1308
Versão da política 1308
Documento da política JSON 1308
Saiba mais 1309
AmazonRoute53ReadOnlyAccess 1309
Utilização desta política 1310
Detalhes desta política 1310
Versão da política 1310
Documento da política JSON 1310
Saiba mais 1311
AmazonRoute53RecoveryClusterFullAccess 1311
Utilização desta política 1311
Detalhes desta política 1311
Versão da política 1311
Documento da política JSON 1311
Saiba mais 1312
AmazonRoute53RecoveryClusterReadOnlyAccess 1312
Utilização desta política 1312
Detalhes desta política 1312
Versão da política 1313
Documento da política JSON 1313
Saiba mais 1313
AmazonRoute53RecoveryControlConfigFullAccess 1313
Utilização desta política 1314
Detalhes desta política 1314
Versão da política 1314
Documento da política JSON 1314
Saiba mais 1314
AmazonRoute53RecoveryControlConfigReadOnlyAccess 1315
Utilização desta política 1315
Detalhes desta política 1315
Versão da política 1315
Documento da política JSON 1315
Saiba mais 1316

AmazonRoute53RecoveryReadinessFullAccess 1316
Utilização desta política 1316
Detalhes desta política 1317
Versão da política 1317
Documento da política JSON 1317
Saiba mais 1317
AmazonRoute53RecoveryReadinessReadOnlyAccess 1318
Utilização desta política 1318
Detalhes desta política 1318
Versão da política 1318
Documento da política JSON 1318
Saiba mais 1319
AmazonRoute53ResolverFullAccess 1319
Utilização desta política 1319
Detalhes desta política 1320
Versão da política 1320
Documento da política JSON 1320
Saiba mais 1321
AmazonRoute53ResolverReadOnlyAccess 1321
Utilização desta política 1321
Detalhes desta política 1321
Versão da política 1321
Documento da política JSON 1322
Saiba mais 1322
AmazonS3ExpressFullAccess 1322
Utilização desta política 1322
Detalhes desta política 1323
Versão da política 1323
Documento da política JSON 1323
Saiba mais 1323
AmazonS3ExpressReadOnlyAccess 1324
Utilização desta política 1324
Detalhes desta política 1324
Versão da política 1324
Documento da política JSON 1324
Saiba mais 1325

AmazonS3FilesClientFullAccess 1325
Utilização desta política 1325
Detalhes desta política 1326
Versão da política 1326
Documento da política JSON 1326
Saiba mais 1326
AmazonS3FilesClientReadOnlyAccess 1327
Utilização desta política 1327
Detalhes desta política 1327
Versão da política 1327
Documento da política JSON 1327
Saiba mais 1328
AmazonS3FilesClientReadWriteAccess 1328
Utilização desta política 1328
Detalhes desta política 1328
Versão da política 1328
Documento da política JSON 1329
Saiba mais 1329
AmazonS3FilesCSIDriverPolicy 1329
Utilização desta política 1329
Detalhes desta política 1329
Versão da política 1330
Documento da política JSON 1330
Saiba mais 1331
AmazonS3FilesFullAccess 1332
Utilização desta política 1332
Detalhes desta política 1332
Versão da política 1332
Documento da política JSON 1332
Saiba mais 1334
AmazonS3FilesReadOnlyAccess 1334
Utilização desta política 1334
Detalhes desta política 1335
Versão da política 1335
Documento da política JSON 1335
Saiba mais 1336

AmazonS3FullAccess 1336
Utilização desta política 1336
Detalhes desta política 1336
Versão da política 1336
Documento da política JSON 1337
Saiba mais 1337
AmazonS3ObjectLambdaExecutionRolePolicy 1337
Utilização desta política 1337
Detalhes desta política 1337
Versão da política 1338
Documento da política JSON 1338
Saiba mais 1338
AmazonS3OutpostsFullAccess 1339
Utilização desta política 1339
Detalhes desta política 1339
Versão da política 1339
Documento da política JSON 1339
Saiba mais 1340
AmazonS3OutpostsReadOnlyAccess 1340
Utilização desta política 1341
Detalhes desta política 1341
Versão da política 1341
Documento da política JSON 1341
Saiba mais 1342
AmazonS3ReadOnlyAccess 1342
Utilização desta política 1342
Detalhes desta política 1343
Versão da política 1343
Documento da política JSON 1343
Saiba mais 1343
AmazonS3TablesFullAccess 1344
Utilização desta política 1344
Detalhes desta política 1344
Versão da política 1344
Documento da política JSON 1344
Saiba mais 1345

AmazonS3TablesLakeFormationServiceRole 1345
Utilização desta política 1345
Detalhes desta política 1345
Versão da política 1346
Documento da política JSON 1346
Saiba mais 1348
AmazonS3TablesReadOnlyAccess 1348
Utilização desta política 1348
Detalhes desta política 1348
Versão da política 1349
Documento da política JSON 1349
Saiba mais 1349
AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy 1350
Utilização desta política 1350
Detalhes desta política 1350
Versão da política 1350
Documento da política JSON 1350
Saiba mais 1362
AmazonSageMakerCanvasAIServicesAccess 1362
Utilização desta política 1362
Detalhes desta política 1362
Versão da política 1363
Documento da política JSON 1363
Saiba mais 1366
AmazonSageMakerCanvasBedrockAccess 1366
Utilização desta política 1366
Detalhes desta política 1366
Versão da política 1366
Documento da política JSON 1367
Saiba mais 1367
AmazonSageMakerCanvasDataPrepFullAccess 1368
Utilização desta política 1368
Detalhes desta política 1368
Versão da política 1368
Documento da política JSON 1368
Saiba mais 1378

AmazonSageMakerCanvasDirectDeployAccess 1378
Utilização desta política 1378
Detalhes desta política 1378
Versão da política 1378
Documento da política JSON 1379
Saiba mais 1379
AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy 1380
Utilização desta política 1380
Detalhes desta política 1380
Versão da política 1380
Documento da política JSON 1380
Saiba mais 1382
AmazonSageMakerCanvasForecastAccess 1382
Utilização desta política 1382
Detalhes desta política 1382
Versão da política 1382
Documento da política JSON 1383
Saiba mais 1383
AmazonSageMakerCanvasFullAccess 1383
Utilização desta política 1384
Detalhes desta política 1384
Versão da política 1384
Documento da política JSON 1384
Saiba mais 1396
AmazonSageMakerCanvasSMDataScienceAssistantAccess 1397
Utilização desta política 1397
Detalhes desta política 1397
Versão da política 1397
Documento da política JSON 1397
Saiba mais 1398
AmazonSageMakerCapacityReservationServiceRolePolicy 1398
Utilização desta política 1399
Detalhes desta política 1399
Versão da política 1399
Documento da política JSON 1399
Saiba mais 1400

AmazonSageMakerClusterInstanceRolePolicy 1400
Utilização desta política 1400
Detalhes desta política 1400
Versão da política 1400
Documento da política JSON 1401
Saiba mais 1402
AmazonSageMakerCoreServiceRolePolicy 1402
Utilização desta política 1403
Detalhes desta política 1403
Versão da política 1403
Documento da política JSON 1403
Saiba mais 1404
AmazonSageMakerEdgeDeviceFleetPolicy 1404
Utilização desta política 1404
Detalhes desta política 1405
Versão da política 1405
Documento da política JSON 1405
Saiba mais 1407
AmazonSageMakerFeatureStoreAccess 1407
Utilização desta política 1407
Detalhes desta política 1407
Versão da política 1407
Documento da política JSON 1408
Saiba mais 1409
AmazonSageMakerFullAccess 1409
Utilização desta política 1409
Detalhes desta política 1409
Versão da política 1409
Documento da política JSON 1410
Saiba mais 1426
AmazonSageMakerGeospatialExecutionRole 1426
Utilização desta política 1426
Detalhes desta política 1426
Versão da política 1427
Documento da política JSON 1427
Saiba mais 1428

AmazonSageMakerGeospatialFullAccess 1428
Utilização desta política 1428
Detalhes desta política 1428
Versão da política 1428
Documento da política JSON 1429
Saiba mais 1429
AmazonSageMakerGroundTruthExecution 1430
Utilização desta política 1430
Detalhes desta política 1430
Versão da política 1430
Documento da política JSON 1430
Saiba mais 1434
AmazonSageMakerHyperPodGatedModelAccess 1434
Utilização desta política 1434
Detalhes desta política 1434
Versão da política 1434
Documento da política JSON 1435
Saiba mais 1435
AmazonSageMakerHyperPodInferenceAccess 1435
Utilização desta política 1436
Detalhes desta política 1436
Versão da política 1436
Documento da política JSON 1436
Saiba mais 1445
AmazonSageMakerHyperPodInferenceGatewayAccess 1445
Utilização desta política 1445
Detalhes desta política 1446
Versão da política 1446
Documento da política JSON 1446
Saiba mais 1447
AmazonSageMakerHyperPodObservabilityAdminAccess 1448
Utilização desta política 1448
Detalhes desta política 1448
Versão da política 1448
Documento da política JSON 1448
Saiba mais 1455

AmazonSageMakerHyperPodServiceRolePolicy 1455
Utilização desta política 1455
Detalhes desta política 1455
Versão da política 1455
Documento da política JSON 1456
Saiba mais 1457
AmazonSageMakerHyperPodTrainingOperatorAccess 1457
Utilização desta política 1457
Detalhes desta política 1457
Versão da política 1457
Documento da política JSON 1458
Saiba mais 1458
AmazonSageMakerInferenceServiceRolePolicy 1458
Utilização desta política 1458
Detalhes desta política 1459
Versão da política 1459
Documento da política JSON 1459
Saiba mais 1462
AmazonSageMakerJobFullAccess 1462
Utilização desta política 1462
Detalhes desta política 1462
Versão da política 1462
Documento da política JSON 1463
Saiba mais 1467
AmazonSageMakerJobRuntimeAccess 1468
Utilização desta política 1468
Detalhes desta política 1468
Versão da política 1468
Documento da política JSON 1468
Saiba mais 1470
AmazonSageMakerMechanicalTurkAccess 1470
Utilização desta política 1470
Detalhes desta política 1470
Versão da política 1470
Documento da política JSON 1470
Saiba mais 1471

AmazonSageMakerModelCustomizationCoreAccess 1471
Utilização desta política 1471
Detalhes desta política 1471
Versão da política 1472
Documento da política JSON 1472
Saiba mais 1483
AmazonSageMakerModelGovernanceUseAccess 1484
Utilização desta política 1484
Detalhes desta política 1484
Versão da política 1484
Documento da política JSON 1484
Saiba mais 1486
AmazonSageMakerModelRegistryFullAccess 1486
Utilização desta política 1487
Detalhes desta política 1487
Versão da política 1487
Documento da política JSON 1487
Saiba mais 1491
AmazonSageMakerNotebooksServiceRolePolicy 1491
Utilização desta política 1491
Detalhes desta política 1491
Versão da política 1491
Documento da política JSON 1492
Saiba mais 1497
AmazonSageMakerPartnerAppsFullAccess 1497
Utilização desta política 1497
Detalhes desta política 1497
Versão da política 1497
Documento da política JSON 1498
Saiba mais 1498
AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy 1499
Utilização desta política 1499
Detalhes desta política 1499
Versão da política 1499
Documento da política JSON 1499
Saiba mais 1500

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy 1500
Utilização desta política 1501
Detalhes desta política 1501
Versão da política 1501
Documento da política JSON 1501
Saiba mais 1505
AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy 1505
Utilização desta política 1505
Detalhes desta política 1505
Versão da política 1505
Documento da política JSON 1506
Saiba mais 1506
AmazonSageMakerPipelinesIntegrations 1506
Utilização desta política 1507
Detalhes desta política 1507
Versão da política 1507
Documento da política JSON 1507
Saiba mais 1509
AmazonSageMakerQuickSightVPCPolicy 1509
Utilização desta política 1509
Detalhes desta política 1509
Versão da política 1510
Documento da política JSON 1510
Saiba mais 1511
AmazonSageMakerReadOnly 1512
Utilização desta política 1512
Detalhes desta política 1512
Versão da política 1512
Documento da política JSON 1512
Saiba mais 1513
AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy 1514
Utilização desta política 1514
Detalhes desta política 1514
Versão da política 1514
Documento da política JSON 1514
Saiba mais 1515

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy 1515
Utilização desta política 1516
Detalhes desta política 1516
Versão da política 1516
Documento da política JSON 1516
Saiba mais 1523
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy 1523
Utilização desta política 1523
Detalhes desta política 1523
Versão da política 1524
Documento da política JSON 1524
Saiba mais 1534
AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy 1534
Utilização desta política 1534
Detalhes desta política 1535
Versão da política 1535
Documento da política JSON 1535
Saiba mais 1538
AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy 1538
Utilização desta política 1538
Detalhes desta política 1538
Versão da política 1539
Documento da política JSON 1539
Saiba mais 1539
AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy 1539
Utilização desta política 1540
Detalhes desta política 1540
Versão da política 1540
Documento da política JSON 1540
Saiba mais 1541
AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy 1541
Utilização desta política 1541
Detalhes desta política 1541
Versão da política 1541
Documento da política JSON 1542
Saiba mais 1544

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy 1544
Utilização desta política 1544
Detalhes desta política 1544
Versão da política 1545
Documento da política JSON 1545
Saiba mais 1555
AmazonSageMakerSpacesControllerPolicy 1555
Utilização desta política 1555
Detalhes desta política 1555
Versão da política 1555
Documento da política JSON 1556
Saiba mais 1560
AmazonSageMakerSpacesRouterPolicy 1560
Utilização desta política 1561
Detalhes desta política 1561
Versão da política 1561
Documento da política JSON 1561
Saiba mais 1562
AmazonSageMakerTrainingPlanCreateAccess 1562
Utilização desta política 1562
Detalhes desta política 1562
Versão da política 1563
Documento da política JSON 1563
Saiba mais 1564
AmazonSecurityLakeAdministrator 1565
Utilização desta política 1565
Detalhes desta política 1565
Versão da política 1565
Documento da política JSON 1565
Saiba mais 1576
AmazonSecurityLakeMetastoreManager 1577
Utilização desta política 1577
Detalhes desta política 1577
Versão da política 1577
Documento da política JSON 1577
Saiba mais 1580

AmazonSecurityLakePermissionsBoundary 1580
Utilização desta política 1580
Detalhes desta política 1580
Versão da política 1580
Documento da política JSON 1581
Saiba mais 1584
AmazonSESFullAccess 1584
Utilização desta política 1584
Detalhes desta política 1584
Versão da política 1584
Documento da política JSON 1585
Saiba mais 1585
AmazonSESReadOnlyAccess 1585
Utilização desta política 1585
Detalhes desta política 1585
Versão da política 1586
Documento da política JSON 1586
Saiba mais 1586
AmazonSESServiceRolePolicy 1587
Utilização desta política 1587
Detalhes desta política 1587
Versão da política 1587
Documento da política JSON 1587
Saiba mais 1588
AmazonSNSFullAccess 1588
Utilização desta política 1588
Detalhes desta política 1588
Versão da política 1588
Documento da política JSON 1589
Saiba mais 1590
AmazonSNSReadOnlyAccess 1590
Utilização desta política 1590
Detalhes desta política 1590
Versão da política 1590
Documento da política JSON 1590
Saiba mais 1591

AmazonSNSRole 1592
Utilização desta política 1592
Detalhes desta política 1592
Versão da política 1592
Documento da política JSON 1592
Saiba mais 1593
AmazonSQSFullAccess 1593
Utilização desta política 1593
Detalhes desta política 1593
Versão da política 1593
Documento da política JSON 1594
Saiba mais 1594
AmazonSQSReadOnlyAccess 1594
Utilização desta política 1594
Detalhes desta política 1595
Versão da política 1595
Documento da política JSON 1595
Saiba mais 1595
AmazonSSMAutomationApproverAccess 1596
Utilização desta política 1596
Detalhes desta política 1596
Versão da política 1596
Documento da política JSON 1596
Saiba mais 1597
AmazonSSMAutomationRole 1597
Utilização desta política 1597
Detalhes desta política 1597
Versão da política 1598
Documento da política JSON 1598
Saiba mais 1599
AmazonSSMDirectoryServiceAccess 1600
Utilização desta política 1600
Detalhes desta política 1600
Versão da política 1600
Documento da política JSON 1600
Saiba mais 1601

AmazonSSMFullAccess 1601
Utilização desta política 1601
Detalhes desta política 1601
Versão da política 1601
Documento da política JSON 1602
Saiba mais 1603
AmazonSSMMaintenanceWindowRole 1603
Utilização desta política 1603
Detalhes desta política 1603
Versão da política 1603
Documento da política JSON 1604
Saiba mais 1605
AmazonSSMManagedEC2InstanceDefaultPolicy 1605
Utilização desta política 1605
Detalhes desta política 1606
Versão da política 1606
Documento da política JSON 1606
Saiba mais 1607
AmazonSSMManagedInstanceCore 1607
Utilização desta política 1608
Detalhes desta política 1608
Versão da política 1608
Documento da política JSON 1608
Saiba mais 1609
AmazonSSMPatchAssociation 1609
Utilização desta política 1610
Detalhes desta política 1610
Versão da política 1610
Documento da política JSON 1610
Saiba mais 1611
AmazonSSMReadOnlyAccess 1611
Utilização desta política 1611
Detalhes desta política 1611
Versão da política 1611
Documento da política JSON 1612
Saiba mais 1612

AmazonSSMServiceRolePolicy 1612
Utilização desta política 1612
Detalhes desta política 1613
Versão da política 1613
Documento da política JSON 1613
Saiba mais 1619
AmazonSumerianFullAccess 1619
Utilização desta política 1619
Detalhes desta política 1619
Versão da política 1619
Documento da política JSON 1619
Saiba mais 1620
AmazonTextractFullAccess 1620
Utilização desta política 1620
Detalhes desta política 1620
Versão da política 1620
Documento da política JSON 1621
Saiba mais 1621
AmazonTextractServiceRole 1621
Utilização desta política 1621
Detalhes desta política 1621
Versão da política 1622
Documento da política JSON 1622
Saiba mais 1622
AmazonTimestreamConsoleFullAccess 1622
Utilização desta política 1623
Detalhes desta política 1623
Versão da política 1623
Documento da política JSON 1623
Saiba mais 1626
AmazonTimestreamFullAccess 1626
Utilização desta política 1626
Detalhes desta política 1626
Versão da política 1626
Documento da política JSON 1627
Saiba mais 1628

AmazonTimestreamInfluxDBFullAccess 1628
Utilização desta política 1628
Detalhes desta política 1628
Versão da política 1629
Documento da política JSON 1629
Saiba mais 1631
AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess 1632
Utilização desta política 1632
Detalhes desta política 1632
Versão da política 1632
Documento da política JSON 1632
Saiba mais 1635
AmazonTimestreamInfluxDBServiceRolePolicy 1635
Utilização desta política 1635
Detalhes desta política 1635
Versão da política 1635
Documento da política JSON 1636
Saiba mais 1639
AmazonTimestreamReadOnlyAccess 1639
Utilização desta política 1639
Detalhes desta política 1639
Versão da política 1639
Documento da política JSON 1640
Saiba mais 1640
AmazonTranscribeFullAccess 1641
Utilização desta política 1641
Detalhes desta política 1641
Versão da política 1641
Documento da política JSON 1641
Saiba mais 1642
AmazonTranscribeReadOnlyAccess 1642
Utilização desta política 1642
Detalhes desta política 1642
Versão da política 1642
Documento da política JSON 1643
Saiba mais 1643

AmazonVerifiedPermissionsFullAccess 1643
Utilização desta política 1643
Detalhes desta política 1644
Versão da política 1644
Documento da política JSON 1644
Saiba mais 1645
AmazonVerifiedPermissionsReadOnlyAccess 1645
Utilização desta política 1645
Detalhes desta política 1645
Versão da política 1645
Documento da política JSON 1646
Saiba mais 1646
AmazonVPCCrossAccountNetworkInterfaceOperations 1647
Utilização desta política 1647
Detalhes desta política 1647
Versão da política 1647
Documento da política JSON 1647
Saiba mais 1649
AmazonVPCFullAccess 1649
Utilização desta política 1649
Detalhes desta política 1649
Versão da política 1649
Documento da política JSON 1650
Saiba mais 1653
AmazonVPCNetworkAccessAnalyzerFullAccessPolicy 1654
Utilização desta política 1654
Detalhes desta política 1654
Versão da política 1654
Documento da política JSON 1654
Saiba mais 1658
AmazonVPCReachabilityAnalyzerFullAccessPolicy 1658
Utilização desta política 1658
Detalhes desta política 1658
Versão da política 1659
Documento da política JSON 1659
Saiba mais 1662

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy 1662
Utilização desta política 1662
Detalhes desta política 1662
Versão da política 1663
Documento da política JSON 1663
Saiba mais 1663
AmazonVPCReadOnlyAccess 1664
Utilização desta política 1664
Detalhes desta política 1664
Versão da política 1664
Documento da política JSON 1664
Saiba mais 1666
AmazonWorkDocsFullAccess 1666
Utilização desta política 1666
Detalhes desta política 1666
Versão da política 1666
Documento da política JSON 1666
Saiba mais 1667
AmazonWorkDocsReadOnlyAccess 1667
Utilização desta política 1667
Detalhes desta política 1667
Versão da política 1668
Documento da política JSON 1668
Saiba mais 1668
AmazonWorkMailEventsServiceRolePolicy 1668
Utilização desta política 1669
Detalhes desta política 1669
Versão da política 1669
Documento da política JSON 1669
Saiba mais 1670
AmazonWorkMailFullAccess 1670
Utilização desta política 1670
Detalhes desta política 1670
Versão da política 1670
Documento da política JSON 1670
Saiba mais 1672

AmazonWorkMailMessageFlowFullAccess 1673
Utilização desta política 1673
Detalhes desta política 1673
Versão da política 1673
Documento da política JSON 1673
Saiba mais 1674
AmazonWorkMailMessageFlowReadOnlyAccess 1674
Utilização desta política 1674
Detalhes desta política 1674
Versão da política 1674
Documento da política JSON 1675
Saiba mais 1675
AmazonWorkMailReadOnlyAccess 1675
Utilização desta política 1675
Detalhes desta política 1675
Versão da política 1676
Documento da política JSON 1676
Saiba mais 1676
AmazonWorkSpacesAdmin 1677
Utilização desta política 1677
Detalhes desta política 1677
Versão da política 1677
Documento da política JSON 1677
Saiba mais 1678
AmazonWorkSpacesApplicationManagerAdminAccess 1679
Utilização desta política 1679
Detalhes desta política 1679
Versão da política 1679
Documento da política JSON 1679
Saiba mais 1680
AmazonWorkspacesPCAAccess 1680
Utilização desta política 1680
Detalhes desta política 1680
Versão da política 1680
Documento da política JSON 1681
Saiba mais 1681

AmazonWorkSpacesPoolServiceAccess 1681
Utilização desta política 1682
Detalhes desta política 1682
Versão da política 1682
Documento da política JSON 1682
Saiba mais 1683
AmazonWorkSpacesSecureBrowserReadOnly 1684
Utilização desta política 1684
Detalhes desta política 1684
Versão da política 1684
Documento da política JSON 1684
Saiba mais 1685
AmazonWorkSpacesSelfServiceAccess 1686
Utilização desta política 1686
Detalhes desta política 1686
Versão da política 1686
Documento da política JSON 1686
Saiba mais 1687
AmazonWorkSpacesServiceAccess 1687
Utilização desta política 1687
Detalhes desta política 1687
Versão da política 1687
Documento da política JSON 1688
Saiba mais 1688
AmazonWorkSpacesThinClientFullAccess 1688
Utilização desta política 1688
Detalhes desta política 1688
Versão da política 1689
Documento da política JSON 1689
Saiba mais 1690
AmazonWorkSpacesThinClientMonitoringServiceRolePolicy 1690
Utilização desta política 1691
Detalhes desta política 1691
Versão da política 1691
Documento da política JSON 1691
Saiba mais 1692

AmazonWorkSpacesThinClientReadOnlyAccess 1692
Utilização desta política 1692
Detalhes desta política 1692
Versão da política 1692
Documento da política JSON 1693
Saiba mais 1694
AmazonWorkSpacesWebReadOnly 1694
Utilização desta política 1694
Detalhes desta política 1694
Versão da política 1695
Documento da política JSON 1695
Saiba mais 1696
AmazonWorkSpacesWebServiceRolePolicy 1696
Utilização desta política 1696
Detalhes desta política 1696
Versão da política 1697
Documento da política JSON 1697
Saiba mais 1699
AmazonZocaloFullAccess 1699
Utilização desta política 1699
Detalhes desta política 1699
Versão da política 1700
Documento da política JSON 1700
Saiba mais 1700
AmazonZocaloReadOnlyAccess 1701
Utilização desta política 1701
Detalhes desta política 1701
Versão da política 1701
Documento da política JSON 1701
Saiba mais 1702
AmplifyBackendDeployFullAccess 1702
Utilização desta política 1702
Detalhes desta política 1702
Versão da política 1702
Documento da política JSON 1703
Saiba mais 1707

AnthropicFullAccess 1707
Utilização desta política 1707
Detalhes desta política 1707
Versão da política 1708
Documento da política JSON 1708
Saiba mais 1710
AnthropicLimitedAccess 1710
Utilização desta política 1710
Detalhes desta política 1710
Versão da política 1710
Documento da política JSON 1710
Saiba mais 1713
AnthropicReadOnlyAccess 1713
Utilização desta política 1713
Detalhes desta política 1713
Versão da política 1713
Documento da política JSON 1714
Saiba mais 1715
AnthropicSelfHostedEnvironmentAccess 1715
Utilização desta política 1716
Detalhes desta política 1716
Versão da política 1716
Documento da política JSON 1716
Saiba mais 1717
APIGatewayServiceRolePolicy 1717
Utilização desta política 1717
Detalhes desta política 1717
Versão da política 1717
Documento da política JSON 1718
Saiba mais 1720
AppIntegrationsServiceLinkedRolePolicy 1720
Utilização desta política 1720
Detalhes desta política 1720
Versão da política 1721
Documento da política JSON 1721
Saiba mais 1722

ApplicationAutoScalingForAmazonAppStreamAccess 1722
Utilização desta política 1723
Detalhes desta política 1723
Versão da política 1723
Documento da política JSON 1723
Saiba mais 1724
ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 1724
Utilização desta política 1724
Detalhes desta política 1724
Versão da política 1725
Documento da política JSON 1725
Saiba mais 1727
AppRunnerNetworkingServiceRolePolicy 1727
Utilização desta política 1727
Detalhes desta política 1727
Versão da política 1727
Documento da política JSON 1728
Saiba mais 1729
AppRunnerServiceRolePolicy 1729
Utilização desta política 1729
Detalhes desta política 1729
Versão da política 1729
Documento da política JSON 1730
Saiba mais 1731
AppStudioServiceRolePolicy 1731
Utilização desta política 1731
Detalhes desta política 1731
Versão da política 1731
Documento da política JSON 1731
Saiba mais 1734
AssuranceServiceRolePolicy 1734
Utilização desta política 1734
Detalhes desta política 1734
Versão da política 1734
Documento da política JSON 1735
Saiba mais 1745

AuroraDsqlServiceLinkedRolePolicy 1745
Utilização desta política 1745
Detalhes desta política 1746
Versão da política 1746
Documento da política JSON 1746
Saiba mais 1747
AutoScalingConsoleFullAccess 1747
Utilização desta política 1747
Detalhes desta política 1747
Versão da política 1747
Documento da política JSON 1747
Saiba mais 1749
AutoScalingConsoleReadOnlyAccess 1749
Utilização desta política 1749
Detalhes desta política 1750
Versão da política 1750
Documento da política JSON 1750
Saiba mais 1751
AutoScalingFullAccess 1751
Utilização desta política 1751
Detalhes desta política 1751
Versão da política 1752
Documento da política JSON 1752
Saiba mais 1753
AutoScalingNotificationAccessRole 1753
Utilização desta política 1754
Detalhes desta política 1754
Versão da política 1754
Documento da política JSON 1754
Saiba mais 1755
AutoScalingReadOnlyAccess 1755
Utilização desta política 1755
Detalhes desta política 1755
Versão da política 1755
Documento da política JSON 1755
Saiba mais 1756

AutoScalingServiceRolePolicy 1756
Utilização desta política 1756
Detalhes desta política 1756
Versão da política 1757
Documento da política JSON 1757
Saiba mais 1760
AWS-SSM-Automation-DiagnosisBucketPolicy 1760
Utilização desta política 1760
Detalhes desta política 1760
Versão da política 1760
Documento da política JSON 1761
Saiba mais 1763
AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy 1763
Utilização desta política 1763
Detalhes desta política 1763
Versão da política 1764
Documento da política JSON 1764
Saiba mais 1766
AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy 1767
Utilização desta política 1767
Detalhes desta política 1767
Versão da política 1767
Documento da política JSON 1767
Saiba mais 1770
AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy 1770
Utilização desta política 1770
Detalhes desta política 1770
Versão da política 1771
Documento da política JSON 1771
Saiba mais 1772
AWS-SSM-RemediationAutomation-AdministrationRolePolicy 1772
Utilização desta política 1772
Detalhes desta política 1772
Versão da política 1772
Documento da política JSON 1773
Saiba mais 1775

AWS-SSM-RemediationAutomation-ExecutionRolePolicy 1775
Utilização desta política 1776
Detalhes desta política 1776
Versão da política 1776
Documento da política JSON 1776
Saiba mais 1782
AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy 1783
Utilização desta política 1783
Detalhes desta política 1783
Versão da política 1783
Documento da política JSON 1783
Saiba mais 1784
AWS_ConfigRole 1784
Utilização desta política 1784
Detalhes desta política 1785
Versão da política 1785
Documento da política JSON 1785
Saiba mais 1844
AWSAccountActivityAccess 1844
Utilização desta política 1844
Detalhes desta política 1844
Versão da política 1844
Documento da política JSON 1844
Saiba mais 1845
AWSAccountManagementFullAccess 1845
Utilização desta política 1845
Detalhes desta política 1846
Versão da política 1846
Documento da política JSON 1846
Saiba mais 1846
AWSAccountManagementReadOnlyAccess 1847
Utilização desta política 1847
Detalhes desta política 1847
Versão da política 1847
Documento da política JSON 1847
Saiba mais 1848

AWSAccountSettingsManagementRole 1848
Utilização desta política 1848
Detalhes desta política 1848
Versão da política 1848
Documento da política JSON 1849
Saiba mais 1851
AWSAccountUsageReportAccess 1852
Utilização desta política 1852
Detalhes desta política 1852
Versão da política 1852
Documento da política JSON 1852
Saiba mais 1853
AWSAgentlessDiscoveryService 1853
Utilização desta política 1853
Detalhes desta política 1853
Versão da política 1853
Documento da política JSON 1853
Saiba mais 1855
AWSAgentRegistryServiceRolePolicy 1855
Utilização desta política 1856
Detalhes desta política 1856
Versão da política 1856
Documento da política JSON 1856
Saiba mais 1858
AWSAppConfigServiceRolePolicy 1859
Utilização desta política 1859
Detalhes desta política 1859
Versão da política 1859
Documento da política JSON 1859
Saiba mais 1860
AWSAppFabricFullAccess 1860
Utilização desta política 1860
Detalhes desta política 1860
Versão da política 1860
Documento da política JSON 1861
Saiba mais 1862

AWSAppFabricReadOnlyAccess 1862
Utilização desta política 1862
Detalhes desta política 1862
Versão da política 1863
Documento da política JSON 1863
Saiba mais 1863
AWSAppFabricServiceRolePolicy 1864
Utilização desta política 1864
Detalhes desta política 1864
Versão da política 1864
Documento da política JSON 1864
Saiba mais 1865
AWSApplicationAutoscalingAppStreamFleetPolicy 1866
Utilização desta política 1866
Detalhes desta política 1866
Versão da política 1866
Documento da política JSON 1866
Saiba mais 1867
AWSApplicationAutoscalingCassandraTablePolicy 1867
Utilização desta política 1867
Detalhes desta política 1867
Versão da política 1868
Documento da política JSON 1868
Saiba mais 1868
AWSApplicationAutoscalingComprehendEndpointPolicy 1869
Utilização desta política 1869
Detalhes desta política 1869
Versão da política 1869
Documento da política JSON 1869
Saiba mais 1870
AWSApplicationAutoScalingCustomResourcePolicy 1870
Utilização desta política 1870
Detalhes desta política 1870
Versão da política 1871
Documento da política JSON 1871
Saiba mais 1871

AWSApplicationAutoscalingDynamoDBTablePolicy 1871
Utilização desta política 1872
Detalhes desta política 1872
Versão da política 1872
Documento da política JSON 1872
Saiba mais 1873
AWSApplicationAutoscalingEC2SpotFleetRequestPolicy 1873
Utilização desta política 1873
Detalhes desta política 1873
Versão da política 1873
Documento da política JSON 1874
Saiba mais 1874
AWSApplicationAutoscalingECSServicePolicy 1874
Utilização desta política 1874
Detalhes desta política 1875
Versão da política 1875
Documento da política JSON 1875
Saiba mais 1876
AWSApplicationAutoscalingElastiCacheRGPolicy 1876
Utilização desta política 1876
Detalhes desta política 1876
Versão da política 1876
Documento da política JSON 1876
Saiba mais 1878
AWSApplicationAutoscalingEMRInstanceGroupPolicy 1878
Utilização desta política 1878
Detalhes desta política 1878
Versão da política 1878
Documento da política JSON 1878
Saiba mais 1879
AWSApplicationAutoscalingKafkaClusterPolicy 1879
Utilização desta política 1879
Detalhes desta política 1879
Versão da política 1880
Documento da política JSON 1880
Saiba mais 1880

AWSApplicationAutoscalingLambdaConcurrencyPolicy 1881
Utilização desta política 1881
Detalhes desta política 1881
Versão da política 1881
Documento da política JSON 1881
Saiba mais 1882
AWSApplicationAutoscalingNeptuneClusterPolicy 1882
Utilização desta política 1882
Detalhes desta política 1882
Versão da política 1883
Documento da política JSON 1883
Saiba mais 1884
AWSApplicationAutoscalingRDSClusterPolicy 1884
Utilização desta política 1885
Detalhes desta política 1885
Versão da política 1885
Documento da política JSON 1885
Saiba mais 1886
AWSApplicationAutoscalingSageMakerEndpointPolicy 1886
Utilização desta política 1886
Detalhes desta política 1886
Versão da política 1887
Documento da política JSON 1887
Saiba mais 1888
AWSApplicationAutoscalingWorkSpacesPoolPolicy 1888
Utilização desta política 1888
Detalhes desta política 1888
Versão da política 1888
Documento da política JSON 1889
Saiba mais 1890
AWSApplicationDiscoveryAgentAccess 1890
Utilização desta política 1890
Detalhes desta política 1890
Versão da política 1891
Documento da política JSON 1891
Saiba mais 1891

AWSApplicationDiscoveryAgentlessCollectorAccess 1892
Utilização desta política 1892
Detalhes desta política 1892
Versão da política 1892
Documento da política JSON 1892
Saiba mais 1893
AWSApplicationDiscoveryServiceFullAccess 1894
Utilização desta política 1894
Detalhes desta política 1894
Versão da política 1894
Documento da política JSON 1894
Saiba mais 1896
AWSApplicationMigrationAgentInstallationPolicy 1896
Utilização desta política 1896
Detalhes desta política 1896
Versão da política 1896
Documento da política JSON 1897
Saiba mais 1898
AWSApplicationMigrationAgentPolicy 1898
Utilização desta política 1898
Detalhes desta política 1898
Versão da política 1898
Documento da política JSON 1899
Saiba mais 1899
AWSApplicationMigrationAgentPolicy_v2 1900
Utilização desta política 1900
Detalhes desta política 1900
Versão da política 1900
Documento da política JSON 1900
Saiba mais 1901
AWSApplicationMigrationConversionServerPolicy 1901
Utilização desta política 1902
Detalhes desta política 1902
Versão da política 1902
Documento da política JSON 1902
Saiba mais 1903

AWSApplicationMigrationEC2Access 1903
Utilização desta política 1903
Detalhes desta política 1903
Versão da política 1903
Documento da política JSON 1904
Saiba mais 1912
AWSApplicationMigrationFSxProxyPolicy 1912
Utilização desta política 1912
Detalhes desta política 1912
Versão da política 1912
Documento da política JSON 1913
Saiba mais 1915
AWSApplicationMigrationFSxProxyVPCPolicy 1916
Utilização desta política 1916
Detalhes desta política 1916
Versão da política 1916
Documento da política JSON 1916
Saiba mais 1921
AWSApplicationMigrationFullAccess 1921
Utilização desta política 1921
Detalhes desta política 1921
Versão da política 1921
Documento da política JSON 1922
Saiba mais 1930
AWSApplicationMigrationMGHAccess 1930
Utilização desta política 1930
Detalhes desta política 1930
Versão da política 1931
Documento da política JSON 1931
Saiba mais 1931
AWSApplicationMigrationNetworkMigrationCustomResource 1932
Utilização desta política 1932
Detalhes desta política 1932
Versão da política 1932
Documento da política JSON 1932
Saiba mais 1933

AWSApplicationMigrationNetworkMigrationMultiAccount 1933
Utilização desta política 1933
Detalhes desta política 1933
Versão da política 1934
Documento da política JSON 1934
Saiba mais 1959
AWSApplicationMigrationReadOnlyAccess 1959
Utilização desta política 1960
Detalhes desta política 1960
Versão da política 1960
Documento da política JSON 1960
Saiba mais 1961
AWSApplicationMigrationReplicationServerPolicy 1962
Utilização desta política 1962
Detalhes desta política 1962
Versão da política 1962
Documento da política JSON 1963
Saiba mais 1964
AWSApplicationMigrationServiceEc2InstancePolicy 1964
Utilização desta política 1965
Detalhes desta política 1965
Versão da política 1965
Documento da política JSON 1965
Saiba mais 1966
AWSApplicationMigrationServiceRolePolicy 1967
Utilização desta política 1967
Detalhes desta política 1967
Versão da política 1967
Documento da política JSON 1967
Saiba mais 1975
AWSApplicationMigrationSSMAccess 1975
Utilização desta política 1975
Detalhes desta política 1975
Versão da política 1975
Documento da política JSON 1976
Saiba mais 1977

AWSApplicationMigrationVCenterClientPolicy 1978
Utilização desta política 1978
Detalhes desta política 1978
Versão da política 1978
Documento da política JSON 1978
Saiba mais 1979
AWSAppMeshEnvoyAccess 1979
Utilização desta política 1979
Detalhes desta política 1979
Versão da política 1980
Documento da política JSON 1980
Saiba mais 1980
AWSAppMeshFullAccess 1980
Utilização desta política 1981
Detalhes desta política 1981
Versão da política 1981
Documento da política JSON 1981
Saiba mais 1982
AWSAppMeshPreviewEnvoyAccess 1983
Utilização desta política 1983
Detalhes desta política 1983
Versão da política 1983
Documento da política JSON 1983
Saiba mais 1984
AWSAppMeshPreviewServiceRolePolicy 1984
Utilização desta política 1984
Detalhes desta política 1984
Versão da política 1984
Documento da política JSON 1985
Saiba mais 1985
AWSAppMeshReadOnly 1985
Utilização desta política 1986
Detalhes desta política 1986
Versão da política 1986
Documento da política JSON 1986
Saiba mais 1987

AWSAppMeshServiceRolePolicy 1987
Utilização desta política 1987
Detalhes desta política 1988
Versão da política 1988
Documento da política JSON 1988
Saiba mais 1989
AWSAppRunnerFullAccess 1989
Utilização desta política 1989
Detalhes desta política 1989
Versão da política 1989
Documento da política JSON 1989
Saiba mais 1990
AWSAppRunnerReadOnlyAccess 1990
Utilização desta política 1991
Detalhes desta política 1991
Versão da política 1991
Documento da política JSON 1991
Saiba mais 1991
AWSAppRunnerServicePolicyForECRAccess 1992
Utilização desta política 1992
Detalhes desta política 1992
Versão da política 1992
Documento da política JSON 1992
Saiba mais 1993
AWSAppSyncAdministrator 1993
Utilização desta política 1993
Detalhes desta política 1993
Versão da política 1994
Documento da política JSON 1994
Saiba mais 1995
AWSAppSyncInvokeFullAccess 1995
Utilização desta política 1995
Detalhes desta política 1995
Versão da política 1996
Documento da política JSON 1996
Saiba mais 1996

AWSAppSyncPushToCloudWatchLogs 1996
Utilização desta política 1997
Detalhes desta política 1997
Versão da política 1997
Documento da política JSON 1997
Saiba mais 1997
AWSAppSyncSchemaAuthor 1998
Utilização desta política 1998
Detalhes desta política 1998
Versão da política 1998
Documento da política JSON 1998
Saiba mais 1999
AWSAppSyncServiceRolePolicy 2000
Utilização desta política 2000
Detalhes desta política 2000
Versão da política 2000
Documento da política JSON 2000
Saiba mais 2001
AWSArtifactAccountSync 2001
Utilização desta política 2001
Detalhes desta política 2001
Versão da política 2001
Documento da política JSON 2002
Saiba mais 2002
AWSArtifactAgreementsFullAccess 2002
Utilização desta política 2002
Detalhes desta política 2003
Versão da política 2003
Documento da política JSON 2003
Saiba mais 2005
AWSArtifactAgreementsReadOnlyAccess 2005
Utilização desta política 2005
Detalhes desta política 2006
Versão da política 2006
Documento da política JSON 2006
Saiba mais 2007

AWSArtifactComplianceInquiriesFullAccess 2007
Utilização desta política 2007
Detalhes desta política 2007
Versão da política 2008
Documento da política JSON 2008
Saiba mais 2009
AWSArtifactComplianceInquiriesReadOnlyAccess 2009
Utilização desta política 2009
Detalhes desta política 2009
Versão da política 2010
Documento da política JSON 2010
Saiba mais 2010
AWSArtifactReportsReadOnlyAccess 2011
Utilização desta política 2011
Detalhes desta política 2011
Versão da política 2011
Documento da política JSON 2011
Saiba mais 2012
AWSArtifactServiceRolePolicy 2012
Utilização desta política 2012
Detalhes desta política 2012
Versão da política 2013
Documento da política JSON 2013
Saiba mais 2013
AWSAuditManagerAdministratorAccess 2013
Utilização desta política 2014
Detalhes desta política 2014
Versão da política 2014
Documento da política JSON 2014
Saiba mais 2018
AWSAuditManagerServiceRolePolicy 2018
Utilização desta política 2019
Detalhes desta política 2019
Versão da política 2019
Documento da política JSON 2019
Saiba mais 2026

AWSAutoScalingPlansEC2AutoScalingPolicy 2026
Utilização desta política 2026
Detalhes desta política 2026
Versão da política 2027
Documento da política JSON 2027
Saiba mais 2027
AWSBackupAccessPointOperatorAccess 2027
Utilização desta política 2028
Detalhes desta política 2028
Versão da política 2028
Documento da política JSON 2028
Saiba mais 2030
AWSBackupAuditAccess 2030
Utilização desta política 2030
Detalhes desta política 2030
Versão da política 2030
Documento da política JSON 2031
Saiba mais 2032
AWSBackupDataTransferAccess 2032
Utilização desta política 2032
Detalhes desta política 2032
Versão da política 2033
Documento da política JSON 2033
Saiba mais 2033
AWSBackupFullAccess 2034
Utilização desta política 2034
Detalhes desta política 2034
Versão da política 2034
Documento da política JSON 2034
Saiba mais 2046
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 2046
Utilização desta política 2046
Detalhes desta política 2046
Versão da política 2047
Documento da política JSON 2047
Saiba mais 2048

AWSBackupGuardDutyRolePolicyForScans 2048
Utilização desta política 2048
Detalhes desta política 2048
Versão da política 2048
Documento da política JSON 2048
Saiba mais 2052
AWSBackupOperatorAccess 2053
Utilização desta política 2053
Detalhes desta política 2053
Versão da política 2053
Documento da política JSON 2053
Saiba mais 2062
AWSBackupOrganizationAdminAccess 2063
Utilização desta política 2063
Detalhes desta política 2063
Versão da política 2063
Documento da política JSON 2063
Saiba mais 2065
AWSBackupRestoreAccessForSAPHANA 2065
Utilização desta política 2065
Detalhes desta política 2066
Versão da política 2066
Documento da política JSON 2066
Saiba mais 2067
AWSBackupSearchOperatorAccess 2067
Utilização desta política 2067
Detalhes desta política 2067
Versão da política 2068
Documento da política JSON 2068
Saiba mais 2069
AWSBackupServiceLinkedRolePolicyForBackup 2070
Utilização desta política 2070
Detalhes desta política 2070
Versão da política 2070
Documento da política JSON 2070
Saiba mais 2080

AWSBackupServiceLinkedRolePolicyForBackupTest 2081
Utilização desta política 2081
Detalhes desta política 2081
Versão da política 2081
Documento da política JSON 2081
Saiba mais 2082
AWSBackupServiceRolePolicyForBackup 2082
Utilização desta política 2082
Detalhes desta política 2082
Versão da política 2083
Documento da política JSON 2083
Saiba mais 2097
AWSBackupServiceRolePolicyForIndexing 2098
Utilização desta política 2098
Detalhes desta política 2098
Versão da política 2098
Documento da política JSON 2098
Saiba mais 2099
AWSBackupServiceRolePolicyForItemRestores 2100
Utilização desta política 2100
Detalhes desta política 2100
Versão da política 2100
Documento da política JSON 2100
Saiba mais 2102
AWSBackupServiceRolePolicyForRestores 2102
Utilização desta política 2103
Detalhes desta política 2103
Versão da política 2103
Documento da política JSON 2103
Saiba mais 2117
AWSBackupServiceRolePolicyForS3Backup 2117
Utilização desta política 2117
Detalhes desta política 2117
Versão da política 2118
Documento da política JSON 2118
Saiba mais 2120

AWSBackupServiceRolePolicyForS3Restore 2121
Utilização desta política 2121
Detalhes desta política 2121
Versão da política 2121
Documento da política JSON 2121
Saiba mais 2123
AWSBackupServiceRolePolicyForScans 2123
Utilização desta política 2123
Detalhes desta política 2123
Versão da política 2123
Documento da política JSON 2124
Saiba mais 2125
AWSBatchFullAccess 2125
Utilização desta política 2125
Detalhes desta política 2125
Versão da política 2125
Documento da política JSON 2125
Saiba mais 2127
AWSBatchServiceEventTargetRole 2127
Utilização desta política 2127
Detalhes desta política 2127
Versão da política 2127
Documento da política JSON 2128
Saiba mais 2128
AWSBatchServiceRole 2128
Utilização desta política 2128
Detalhes desta política 2129
Versão da política 2129
Documento da política JSON 2129
Saiba mais 2132
AWSBatchServiceRolePolicyForSageMaker 2132
Utilização desta política 2133
Detalhes desta política 2133
Versão da política 2133
Documento da política JSON 2133
Saiba mais 2135

AWSBCMDataExportsServiceRolePolicy 2135
Utilização desta política 2135
Detalhes desta política 2135
Versão da política 2135
Documento da política JSON 2136
Saiba mais 2136
AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy 2136
Utilização desta política 2136
Detalhes desta política 2136
Versão da política 2137
Documento da política JSON 2137
Saiba mais 2139
AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy 2139
Utilização desta política 2139
Detalhes desta política 2139
Versão da política 2139
Documento da política JSON 2140
Saiba mais 2141
AWSBedrockAgentCoreRuntimeInstancesServiceRolePolicy 2141
Utilização desta política 2142
Detalhes desta política 2142
Versão da política 2142
Documento da política JSON 2142
Saiba mais 2145
AWSBillingConductorFullAccess 2145
Utilização desta política 2145
Detalhes desta política 2145
Versão da política 2145
Documento da política JSON 2146
Saiba mais 2146
AWSBillingConductorReadOnlyAccess 2146
Utilização desta política 2147
Detalhes desta política 2147
Versão da política 2147
Documento da política JSON 2147
Saiba mais 2148

AWSBillingConductorRolePolicy 2148
Utilização desta política 2148
Detalhes desta política 2148
Versão da política 2149
Documento da política JSON 2149
Saiba mais 2149
AWSBillingReadOnlyAccess 2150
Utilização desta política 2150
Detalhes desta política 2150
Versão da política 2150
Documento da política JSON 2150
Saiba mais 2152
AWSBillingServiceRolePolicy 2153
Utilização desta política 2153
Detalhes desta política 2153
Versão da política 2153
Documento da política JSON 2153
Saiba mais 2154
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM 2154
Utilização desta política 2154
Detalhes desta política 2154
Versão da política 2154
Documento da política JSON 2155
Saiba mais 2156
AWSBudgetsActionsWithAWSResourceControlAccess 2156
Utilização desta política 2156
Detalhes desta política 2156
Versão da política 2156
Documento da política JSON 2157
Saiba mais 2158
AWSBudgetsReadOnlyAccess 2158
Utilização desta política 2158
Detalhes desta política 2158
Versão da política 2159
Documento da política JSON 2159
Saiba mais 2159

AWSBudgetsSpendLimitMemberRolePolicy 2159
Utilização desta política 2160
Detalhes desta política 2160
Versão da política 2160
Documento da política JSON 2160
Saiba mais 2166
AWSBugBustFullAccess 2166
Utilização desta política 2166
Detalhes desta política 2166
Versão da política 2167
Documento da política JSON 2167
Saiba mais 2168
AWSBugBustPlayerAccess 2168
Utilização desta política 2168
Detalhes desta política 2168
Versão da política 2169
Documento da política JSON 2169
Saiba mais 2170
AWSBugBustServiceRolePolicy 2170
Utilização desta política 2170
Detalhes desta política 2170
Versão da política 2170
Documento da política JSON 2171
Saiba mais 2171
AWSCertificateManagerFullAccess 2171
Utilização desta política 2171
Detalhes desta política 2172
Versão da política 2172
Documento da política JSON 2172
Saiba mais 2173
AWSCertificateManagerPrivateCAAuditor 2173
Utilização desta política 2173
Detalhes desta política 2173
Versão da política 2174
Documento da política JSON 2174
Saiba mais 2174

AWSCertificateManagerPrivateCAFullAccess 2175
Utilização desta política 2175
Detalhes desta política 2175
Versão da política 2175
Documento da política JSON 2175
Saiba mais 2176
AWSCertificateManagerPrivateCAPrivilegedUser 2176
Utilização desta política 2176
Detalhes desta política 2176
Versão da política 2176
Documento da política JSON 2177
Saiba mais 2178
AWSCertificateManagerPrivateCAReadOnly 2178
Utilização desta política 2178
Detalhes desta política 2178
Versão da política 2179
Documento da política JSON 2179
Saiba mais 2179
AWSCertificateManagerPrivateCAUser 2180
Utilização desta política 2180
Detalhes desta política 2180
Versão da política 2180
Documento da política JSON 2180
Saiba mais 2181
AWSCertificateManagerReadOnly 2182
Utilização desta política 2182
Detalhes desta política 2182
Versão da política 2182
Documento da política JSON 2182
Saiba mais 2183
AWSChatbotServiceLinkedRolePolicy 2183
Utilização desta política 2183
Detalhes desta política 2183
Versão da política 2184
Documento da política JSON 2184
Saiba mais 2185

AWSCleanRoomsFullAccess 2185
Utilização desta política 2185
Detalhes desta política 2185
Versão da política 2185
Documento da política JSON 2185
Saiba mais 2190
AWSCleanRoomsFullAccessNoQuerying 2190
Utilização desta política 2190
Detalhes desta política 2190
Versão da política 2190
Documento da política JSON 2191
Saiba mais 2195
AWSCleanRoomsMLFullAccess 2196
Utilização desta política 2196
Detalhes desta política 2196
Versão da política 2196
Documento da política JSON 2196
Saiba mais 2200
AWSCleanRoomsMLReadOnlyAccess 2200
Utilização desta política 2201
Detalhes desta política 2201
Versão da política 2201
Documento da política JSON 2201
Saiba mais 2202
AWSCleanRoomsReadOnlyAccess 2202
Utilização desta política 2203
Detalhes desta política 2203
Versão da política 2203
Documento da política JSON 2203
Saiba mais 2204
AWSCleanRoomsServiceRolePolicy 2205
Utilização desta política 2205
Detalhes desta política 2205
Versão da política 2205
Documento da política JSON 2205
Saiba mais 2206

AWSCloud9Administrator 2206
Utilização desta política 2206
Detalhes desta política 2206
Versão da política 2206
Documento da política JSON 2207
Saiba mais 2208
AWSCloud9EnvironmentMember 2208
Utilização desta política 2209
Detalhes desta política 2209
Versão da política 2209
Documento da política JSON 2209
Saiba mais 2211
AWSCloud9ServiceRolePolicy 2211
Utilização desta política 2211
Detalhes desta política 2211
Versão da política 2211
Documento da política JSON 2212
Saiba mais 2214
AWSCloud9SSMInstanceProfile 2214
Utilização desta política 2215
Detalhes desta política 2215
Versão da política 2215
Documento da política JSON 2215
Saiba mais 2216
AWSCloud9User 2216
Utilização desta política 2216
Detalhes desta política 2216
Versão da política 2216
Documento da política JSON 2216
Saiba mais 2219
AWSCloudFormationFullAccess 2219
Utilização desta política 2219
Detalhes desta política 2219
Versão da política 2220
Documento da política JSON 2220
Saiba mais 2220

AWSCloudFormationReadOnlyAccess 2220
Utilização desta política 2221
Detalhes desta política 2221
Versão da política 2221
Documento da política JSON 2221
Saiba mais 2222
AWSCloudFrontLogger 2222
Utilização desta política 2222
Detalhes desta política 2222
Versão da política 2222
Documento da política JSON 2222
Saiba mais 2223
AWSCloudFrontVPCOriginServiceRolePolicy 2223
Utilização desta política 2223
Detalhes desta política 2223
Versão da política 2224
Documento da política JSON 2224
Saiba mais 2226
AWSCloudHSMFullAccess 2227
Utilização desta política 2227
Detalhes desta política 2227
Versão da política 2227
Documento da política JSON 2227
Saiba mais 2228
AWSCloudHSMReadOnlyAccess 2228
Utilização desta política 2228
Detalhes desta política 2228
Versão da política 2228
Documento da política JSON 2228
Saiba mais 2229
AWSCloudHSMRole 2229
Utilização desta política 2229
Detalhes desta política 2229
Versão da política 2229
Documento da política JSON 2230
Saiba mais 2230

AWSCloudMapDiscoverInstanceAccess 2230
Utilização desta política 2231
Detalhes desta política 2231
Versão da política 2231
Documento da política JSON 2231
Saiba mais 2232
AWSCloudMapFullAccess 2232
Utilização desta política 2232
Detalhes desta política 2232
Versão da política 2232
Documento da política JSON 2232
Saiba mais 2233
AWSCloudMapReadOnlyAccess 2233
Utilização desta política 2233
Detalhes desta política 2234
Versão da política 2234
Documento da política JSON 2234
Saiba mais 2234
AWSCloudMapRegisterInstanceAccess 2235
Utilização desta política 2235
Detalhes desta política 2235
Versão da política 2235
Documento da política JSON 2235
Saiba mais 2236
AWSCloudShellFullAccess 2236
Utilização desta política 2236
Detalhes desta política 2236
Versão da política 2237
Documento da política JSON 2237
Saiba mais 2237
AWSCloudTrail_FullAccess 2237
Utilização desta política 2238
Detalhes desta política 2238
Versão da política 2238
Documento da política JSON 2238
Saiba mais 2241

AWSCloudTrail_ReadOnlyAccess 2241
Utilização desta política 2241
Detalhes desta política 2241
Versão da política 2241
Documento da política JSON 2241
Saiba mais 2242
AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy 2242
Utilização desta política 2242
Detalhes desta política 2242
Versão da política 2243
Documento da política JSON 2243
Saiba mais 2243
AWSCloudWatchOmniServiceRolePolicy 2243
Utilização desta política 2244
Detalhes desta política 2244
Versão da política 2244
Documento da política JSON 2244
Saiba mais 2248
AWSCodeArtifactAdminAccess 2248
Utilização desta política 2248
Detalhes desta política 2248
Versão da política 2249
Documento da política JSON 2249
Saiba mais 2249
AWSCodeArtifactReadOnlyAccess 2250
Utilização desta política 2250
Detalhes desta política 2250
Versão da política 2250
Documento da política JSON 2250
Saiba mais 2251
AWSCodeBuildAdminAccess 2251
Utilização desta política 2251
Detalhes desta política 2251
Versão da política 2252
Documento da política JSON 2252
Saiba mais 2255

AWSCodeBuildDeveloperAccess 2256
Utilização desta política 2256
Detalhes desta política 2256
Versão da política 2256
Documento da política JSON 2256
Saiba mais 2259
AWSCodeBuildReadOnlyAccess 2259
Utilização desta política 2259
Detalhes desta política 2260
Versão da política 2260
Documento da política JSON 2260
Saiba mais 2261
AWSCodeCommitFullAccess 2262
Utilização desta política 2262
Detalhes desta política 2262
Versão da política 2262
Documento da política JSON 2262
Saiba mais 2267
AWSCodeCommitPowerUser 2267
Utilização desta política 2267
Detalhes desta política 2267
Versão da política 2268
Documento da política JSON 2268
Saiba mais 2273
AWSCodeCommitReadOnly 2273
Utilização desta política 2273
Detalhes desta política 2273
Versão da política 2273
Documento da política JSON 2273
Saiba mais 2276
AWSCodeDeployDeployerAccess 2276
Utilização desta política 2276
Detalhes desta política 2276
Versão da política 2277
Documento da política JSON 2277
Saiba mais 2278

AWSCodeDeployFullAccess 2279
Utilização desta política 2279
Detalhes desta política 2279
Versão da política 2279
Documento da política JSON 2279
Saiba mais 2281
AWSCodeDeployReadOnlyAccess 2281
Utilização desta política 2281
Detalhes desta política 2281
Versão da política 2281
Documento da política JSON 2282
Saiba mais 2283
AWSCodeDeployRole 2283
Utilização desta política 2283
Detalhes desta política 2283
Versão da política 2283
Documento da política JSON 2284
Saiba mais 2285
AWSCodeDeployRoleForCloudFormation 2285
Utilização desta política 2285
Detalhes desta política 2285
Versão da política 2286
Documento da política JSON 2286
Saiba mais 2286
AWSCodeDeployRoleForECS 2286
Utilização desta política 2287
Detalhes desta política 2287
Versão da política 2287
Documento da política JSON 2287
Saiba mais 2288
AWSCodeDeployRoleForECSLimited 2288
Utilização desta política 2288
Detalhes desta política 2289
Versão da política 2289
Documento da política JSON 2289
Saiba mais 2291

AWSCodeDeployRoleForLambda 2291
Utilização desta política 2291
Detalhes desta política 2291
Versão da política 2291
Documento da política JSON 2292
Saiba mais 2293
AWSCodeDeployRoleForLambdaLimited 2293
Utilização desta política 2293
Detalhes desta política 2293
Versão da política 2293
Documento da política JSON 2294
Saiba mais 2295
AWSCodePipeline_FullAccess 2295
Utilização desta política 2295
Detalhes desta política 2295
Versão da política 2295
Documento da política JSON 2296
Saiba mais 2299
AWSCodePipeline_ReadOnlyAccess 2300
Utilização desta política 2300
Detalhes desta política 2300
Versão da política 2300
Documento da política JSON 2300
Saiba mais 2301
AWSCodePipelineApproverAccess 2302
Utilização desta política 2302
Detalhes desta política 2302
Versão da política 2302
Documento da política JSON 2302
Saiba mais 2303
AWSCodePipelineCustomActionAccess 2303
Utilização desta política 2303
Detalhes desta política 2303
Versão da política 2303
Documento da política JSON 2304
Saiba mais 2304

AWSCodeStarFullAccess 2304
Utilização desta política 2304
Detalhes desta política 2305
Versão da política 2305
Documento da política JSON 2305
Saiba mais 2306
AWSCodeStarNotificationsServiceRolePolicy 2306
Utilização desta política 2306
Detalhes desta política 2306
Versão da política 2307
Documento da política JSON 2307
Saiba mais 2308
AWSCodeStarServiceRole 2308
Utilização desta política 2308
Detalhes desta política 2308
Versão da política 2308
Documento da política JSON 2309
Saiba mais 2314
AWSCompromisedKeyQuarantine 2314
Utilização desta política 2314
Detalhes desta política 2314
Versão da política 2315
Documento da política JSON 2315
Saiba mais 2316
AWSCompromisedKeyQuarantineV2 2316
Utilização desta política 2316
Detalhes desta política 2316
Versão da política 2317
Documento da política JSON 2317
Saiba mais 2319
AWSCompromisedKeyQuarantineV3 2320
Utilização desta política 2320
Detalhes desta política 2320
Versão da política 2320
Documento da política JSON 2320
Saiba mais 2323

AWSConfigMultiAccountSetupPolicy 2323
Utilização desta política 2324
Detalhes desta política 2324
Versão da política 2324
Documento da política JSON 2324
Saiba mais 2326
AWSConfigRemediationServiceRolePolicy 2326
Utilização desta política 2326
Detalhes desta política 2326
Versão da política 2327
Documento da política JSON 2327
Saiba mais 2328
AWSConfigRoleForOrganizations 2328
Utilização desta política 2328
Detalhes desta política 2328
Versão da política 2328
Documento da política JSON 2328
Saiba mais 2329
AWSConfigRulesExecutionRole 2329
Utilização desta política 2329
Detalhes desta política 2329
Versão da política 2330
Documento da política JSON 2330
Saiba mais 2330
AWSConfigServiceRolePolicy 2331
Utilização desta política 2331
Detalhes desta política 2331
Versão da política 2331
Documento da política JSON 2331
Saiba mais 2391
AWSConfigThirdPartyServiceRolePolicy 2391
Utilização desta política 2391
Detalhes desta política 2391
Versão da política 2391
Documento da política JSON 2392
Saiba mais 2393

AWSConfigUserAccess 2393
Utilização desta política 2393
Detalhes desta política 2393
Versão da política 2393
Documento da política JSON 2393
Saiba mais 2394
AWSConnector 2394
Utilização desta política 2394
Detalhes desta política 2394
Versão da política 2395
Documento da política JSON 2395
Saiba mais 2397
AWSControlTowerAccountServiceRolePolicy 2397
Utilização desta política 2397
Detalhes desta política 2397
Versão da política 2398
Documento da política JSON 2398
Saiba mais 2403
AWSControlTowerCloudTrailRolePolicy 2403
Utilização desta política 2403
Detalhes desta política 2403
Versão da política 2404
Documento da política JSON 2404
Saiba mais 2404
AWSControlTowerIdentityCenterManagementPolicy 2405
Utilização desta política 2405
Detalhes desta política 2405
Versão da política 2405
Documento da política JSON 2405
Saiba mais 2406
AWSControlTowerServiceRolePolicy 2407
Utilização desta política 2407
Detalhes desta política 2407
Versão da política 2407
Documento da política JSON 2407
Saiba mais 2413

AWSCostAndUsageReportAutomationPolicy 2413
Utilização desta política 2413
Detalhes desta política 2413
Versão da política 2414
Documento da política JSON 2414
Saiba mais 2415
AWSDataExchangeDataGrantOwnerFullAccess 2415
Utilização desta política 2415
Detalhes desta política 2415
Versão da política 2415
Documento da política JSON 2416
Saiba mais 2417
AWSDataExchangeDataGrantReceiverFullAccess 2417
Utilização desta política 2418
Detalhes desta política 2418
Versão da política 2418
Documento da política JSON 2418
Saiba mais 2420
AWSDataExchangeFullAccess 2420
Utilização desta política 2420
Detalhes desta política 2420
Versão da política 2420
Documento da política JSON 2420
Saiba mais 2424
AWSDataExchangeProviderFullAccess 2424
Utilização desta política 2424
Detalhes desta política 2424
Versão da política 2425
Documento da política JSON 2425
Saiba mais 2429
AWSDataExchangeReadOnly 2429
Utilização desta política 2429
Detalhes desta política 2429
Versão da política 2429
Documento da política JSON 2430
Saiba mais 2431

AWSDataExchangeServiceRolePolicyForLicenseManagement 2431
Utilização desta política 2431
Detalhes desta política 2431
Versão da política 2432
Documento da política JSON 2432
Saiba mais 2432
AWSDataExchangeServiceRolePolicyForOrganizationDiscovery 2432
Utilização desta política 2433
Detalhes desta política 2433
Versão da política 2433
Documento da política JSON 2433
Saiba mais 2434
AWSDataExchangeSubscriberFullAccess 2434
Utilização desta política 2434
Detalhes desta política 2434
Versão da política 2434
Documento da política JSON 2435
Saiba mais 2437
AWSDataLifecycleManagerServiceRole 2437
Utilização desta política 2437
Detalhes desta política 2437
Versão da política 2438
Documento da política JSON 2438
Saiba mais 2439
AWSDataLifecycleManagerServiceRoleForAMIManagement 2439
Utilização desta política 2439
Detalhes desta política 2439
Versão da política 2440
Documento da política JSON 2440
Saiba mais 2441
AWSDataLifecycleManagerSSMFullAccess 2441
Utilização desta política 2442
Detalhes desta política 2442
Versão da política 2442
Documento da política JSON 2442
Saiba mais 2443

AWSDataPipeline_FullAccess 2444
Utilização desta política 2444
Detalhes desta política 2444
Versão da política 2444
Documento da política JSON 2444
Saiba mais 2445
AWSDataPipeline_PowerUser 2445
Utilização desta política 2446
Detalhes desta política 2446
Versão da política 2446
Documento da política JSON 2446
Saiba mais 2447
AWSDataSyncDiscoveryServiceRolePolicy 2447
Utilização desta política 2447
Detalhes desta política 2447
Versão da política 2448
Documento da política JSON 2448
Saiba mais 2449
AWSDataSyncFullAccess 2449
Utilização desta política 2449
Detalhes desta política 2449
Versão da política 2449
Documento da política JSON 2450
Saiba mais 2452
AWSDataSyncReadOnlyAccess 2452
Utilização desta política 2452
Detalhes desta política 2453
Versão da política 2453
Documento da política JSON 2453
Saiba mais 2454
AWSDataSyncServiceRolePolicy 2454
Utilização desta política 2454
Detalhes desta política 2454
Versão da política 2454
Documento da política JSON 2455
Saiba mais 2456

AWSDeadlineCloud-FleetWorker 2456
Utilização desta política 2456
Detalhes desta política 2456
Versão da política 2456
Documento da política JSON 2456
Saiba mais 2457
AWSDeadlineCloud-UserAccessFarms 2457
Utilização desta política 2457
Detalhes desta política 2458
Versão da política 2458
Documento da política JSON 2458
Saiba mais 2464
AWSDeadlineCloud-UserAccessFleets 2464
Utilização desta política 2465
Detalhes desta política 2465
Versão da política 2465
Documento da política JSON 2465
Saiba mais 2469
AWSDeadlineCloud-UserAccessJobs 2469
Utilização desta política 2469
Detalhes desta política 2469
Versão da política 2469
Documento da política JSON 2470
Saiba mais 2473
AWSDeadlineCloud-UserAccessQueues 2474
Utilização desta política 2474
Detalhes desta política 2474
Versão da política 2474
Documento da política JSON 2474
Saiba mais 2479
AWSDeadlineCloud-WorkerHost 2479
Utilização desta política 2479
Detalhes desta política 2480
Versão da política 2480
Documento da política JSON 2480
Saiba mais 2481

AWSDeepLensLambdaFunctionAccessPolicy 2481
Utilização desta política 2482
Detalhes desta política 2482
Versão da política 2482
Documento da política JSON 2482
Saiba mais 2483
AWSDeepLensServiceRolePolicy 2484
Utilização desta política 2484
Detalhes desta política 2484
Versão da política 2484
Documento da política JSON 2484
Saiba mais 2491
AWSDeepRacerAccountAdminAccess 2492
Utilização desta política 2492
Detalhes desta política 2492
Versão da política 2492
Documento da política JSON 2492
Saiba mais 2493
AWSDeepRacerCloudFormationAccessPolicy 2493
Utilização desta política 2493
Detalhes desta política 2493
Versão da política 2493
Documento da política JSON 2494
Saiba mais 2497
AWSDeepRacerDefaultMultiUserAccess 2497
Utilização desta política 2497
Detalhes desta política 2497
Versão da política 2497
Documento da política JSON 2497
Saiba mais 2499
AWSDeepRacerFullAccess 2499
Utilização desta política 2499
Detalhes desta política 2499
Versão da política 2500
Documento da política JSON 2500
Saiba mais 2501

AWSDeepRacerRoboMakerAccessPolicy 2501
Utilização desta política 2501
Detalhes desta política 2501
Versão da política 2501
Documento da política JSON 2502
Saiba mais 2504
AWSDeepRacerServiceRolePolicy 2504
Utilização desta política 2504
Detalhes desta política 2504
Versão da política 2504
Documento da política JSON 2504
Saiba mais 2508
AWSDenyAll 2508
Utilização desta política 2508
Detalhes desta política 2508
Versão da política 2508
Documento da política JSON 2508
Saiba mais 2509
AWSDeviceFarmFullAccess 2509
Utilização desta política 2509
Detalhes desta política 2509
Versão da política 2509
Documento da política JSON 2510
Saiba mais 2510
AWSDeviceFarmServiceRolePolicy 2510
Utilização desta política 2510
Detalhes desta política 2511
Versão da política 2511
Documento da política JSON 2511
Saiba mais 2513
AWSDeviceFarmTestGridServiceRolePolicy 2513
Utilização desta política 2513
Detalhes desta política 2513
Versão da política 2514
Documento da política JSON 2514
Saiba mais 2516

AWSDirectConnectFullAccess 2516
Utilização desta política 2516
Detalhes desta política 2516
Versão da política 2517
Documento da política JSON 2517
Saiba mais 2517
AWSDirectConnectReadOnlyAccess 2517
Utilização desta política 2518
Detalhes desta política 2518
Versão da política 2518
Documento da política JSON 2518
Saiba mais 2519
AWSDirectConnectServiceRolePolicy 2519
Utilização desta política 2519
Detalhes desta política 2519
Versão da política 2519
Documento da política JSON 2520
Saiba mais 2520
AWSDirectoryServiceDataFullAccess 2520
Utilização desta política 2520
Detalhes desta política 2520
Versão da política 2521
Documento da política JSON 2521
Saiba mais 2522
AWSDirectoryServiceDataReadOnlyAccess 2522
Utilização desta política 2522
Detalhes desta política 2522
Versão da política 2522
Documento da política JSON 2523
Saiba mais 2523
AWSDirectoryServiceFullAccess 2523
Utilização desta política 2524
Detalhes desta política 2524
Versão da política 2524
Documento da política JSON 2524
Saiba mais 2526

AWSDirectoryServiceReadOnlyAccess 2526
Utilização desta política 2526
Detalhes desta política 2526
Versão da política 2527
Documento da política JSON 2527
Saiba mais 2527
AWSDirectoryServiceServiceRolePolicy 2528
Utilização desta política 2528
Detalhes desta política 2528
Versão da política 2528
Documento da política JSON 2528
Saiba mais 2529
AWSDiscoveryContinuousExportFirehosePolicy 2530
Utilização desta política 2530
Detalhes desta política 2530
Versão da política 2530
Documento da política JSON 2530
Saiba mais 2531
AWSDMSFleetAdvisorServiceRolePolicy 2531
Utilização desta política 2532
Detalhes desta política 2532
Versão da política 2532
Documento da política JSON 2532
Saiba mais 2533
AWSDMSServerlessServiceRolePolicy 2533
Utilização desta política 2533
Detalhes desta política 2533
Versão da política 2533
Documento da política JSON 2533
Saiba mais 2536
AWSEC2CapacityManagerServiceRolePolicy 2536
Utilização desta política 2537
Detalhes desta política 2537
Versão da política 2537
Documento da política JSON 2537
Saiba mais 2538

AWSEC2CapacityReservationFleetRolePolicy 2538
Utilização desta política 2538
Detalhes desta política 2538
Versão da política 2539
Documento da política JSON 2539
Saiba mais 2540
AWSEC2FleetServiceRolePolicy 2540
Utilização desta política 2540
Detalhes desta política 2540
Versão da política 2541
Documento da política JSON 2541
Saiba mais 2543
AWSEC2SpotFleetServiceRolePolicy 2543
Utilização desta política 2543
Detalhes desta política 2543
Versão da política 2544
Documento da política JSON 2544
Saiba mais 2546
AWSEC2SpotServiceRolePolicy 2546
Utilização desta política 2546
Detalhes desta política 2546
Versão da política 2546
Documento da política JSON 2546
Saiba mais 2548
AWSEC2SqlHaInstancePolicy 2548
Utilização desta política 2548
Detalhes desta política 2548
Versão da política 2549
Documento da política JSON 2549
Saiba mais 2550
AWSEC2SqlHaServiceRolePolicy 2550
Utilização desta política 2550
Detalhes desta política 2551
Versão da política 2551
Documento da política JSON 2551
Saiba mais 2553

AWSEC2VssRestorePolicy 2553
Utilização desta política 2553
Detalhes desta política 2553
Versão da política 2553
Documento da política JSON 2554
Saiba mais 2556
AWSEC2VssSnapshotPolicy 2556
Utilização desta política 2556
Detalhes desta política 2557
Versão da política 2557
Documento da política JSON 2557
Saiba mais 2560
AWSECRPullThroughCache_ServiceRolePolicy 2560
Utilização desta política 2561
Detalhes desta política 2561
Versão da política 2561
Documento da política JSON 2561
Saiba mais 2562
AWSElasticBeanstalkCustomPlatformforEC2Role 2562
Utilização desta política 2563
Detalhes desta política 2563
Versão da política 2563
Documento da política JSON 2563
Saiba mais 2565
AWSElasticBeanstalkEKSImageBuild 2565
Utilização desta política 2565
Detalhes desta política 2565
Versão da política 2565
Documento da política JSON 2566
Saiba mais 2568
AWSElasticBeanstalkEKSObservability 2568
Utilização desta política 2568
Detalhes desta política 2568
Versão da política 2568
Documento da política JSON 2569
Saiba mais 2570

AWSElasticBeanstalkEKSTagging 2570
Utilização desta política 2571
Detalhes desta política 2571
Versão da política 2571
Documento da política JSON 2571
Saiba mais 2574
AWSElasticBeanstalkEnhancedHealth 2574
Utilização desta política 2574
Detalhes desta política 2574
Versão da política 2574
Documento da política JSON 2574
Saiba mais 2575
AWSElasticBeanstalkMaintenance 2576
Utilização desta política 2576
Detalhes desta política 2576
Versão da política 2576
Documento da política JSON 2576
Saiba mais 2577
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy 2577
Utilização desta política 2578
Detalhes desta política 2578
Versão da política 2578
Documento da política JSON 2578
Saiba mais 2585
AWSElasticBeanstalkManagedUpdatesServiceRolePolicy 2585
Utilização desta política 2586
Detalhes desta política 2586
Versão da política 2586
Documento da política JSON 2586
Saiba mais 2592
AWSElasticBeanstalkMulticontainerDocker 2592
Utilização desta política 2592
Detalhes desta política 2592
Versão da política 2592
Documento da política JSON 2593
Saiba mais 2595

AWSElasticBeanstalkReadOnly 2595
Utilização desta política 2595
Detalhes desta política 2595
Versão da política 2595
Documento da política JSON 2596
Saiba mais 2598
AWSElasticBeanstalkRoleCore 2598
Utilização desta política 2598
Detalhes desta política 2598
Versão da política 2599
Documento da política JSON 2599
Saiba mais 2604
AWSElasticBeanstalkRoleCWL 2604
Utilização desta política 2604
Detalhes desta política 2604
Versão da política 2604
Documento da política JSON 2605
Saiba mais 2605
AWSElasticBeanstalkRoleECS 2605
Utilização desta política 2605
Detalhes desta política 2606
Versão da política 2606
Documento da política JSON 2606
Saiba mais 2607
AWSElasticBeanstalkRoleRDS 2607
Utilização desta política 2607
Detalhes desta política 2607
Versão da política 2608
Documento da política JSON 2608
Saiba mais 2608
AWSElasticBeanstalkRoleSNS 2609
Utilização desta política 2609
Detalhes desta política 2609
Versão da política 2609
Documento da política JSON 2609
Saiba mais 2610

AWSElasticBeanstalkRoleWorkerTier 2610
Utilização desta política 2610
Detalhes desta política 2610
Versão da política 2611
Documento da política JSON 2611
Saiba mais 2612
AWSElasticBeanstalkService 2612
Utilização desta política 2612
Detalhes desta política 2612
Versão da política 2612
Documento da política JSON 2613
Saiba mais 2617
AWSElasticBeanstalkServiceRolePolicy 2617
Utilização desta política 2617
Detalhes desta política 2617
Versão da política 2618
Documento da política JSON 2618
Saiba mais 2631
AWSElasticBeanstalkWebTier 2632
Utilização desta política 2632
Detalhes desta política 2632
Versão da política 2632
Documento da política JSON 2632
Saiba mais 2635
AWSElasticBeanstalkWorkerTier 2635
Utilização desta política 2635
Detalhes desta política 2635
Versão da política 2635
Documento da política JSON 2636
Saiba mais 2639
AWSElasticDisasterRecoveryAgentInstallationPolicy 2639
Utilização desta política 2639
Detalhes desta política 2639
Versão da política 2639
Documento da política JSON 2640
Saiba mais 2641

AWSElasticDisasterRecoveryAgentPolicy 2641
Utilização desta política 2642
Detalhes desta política 2642
Versão da política 2642
Documento da política JSON 2642
Saiba mais 2643
AWSElasticDisasterRecoveryConsoleFullAccess 2643
Utilização desta política 2643
Detalhes desta política 2643
Versão da política 2644
Documento da política JSON 2644
Saiba mais 2654
AWSElasticDisasterRecoveryConsoleFullAccess_v2 2654
Utilização desta política 2654
Detalhes desta política 2654
Versão da política 2655
Documento da política JSON 2655
Saiba mais 2670
AWSElasticDisasterRecoveryConversionServerPolicy 2671
Utilização desta política 2671
Detalhes desta política 2671
Versão da política 2671
Documento da política JSON 2672
Saiba mais 2672
AWSElasticDisasterRecoveryCrossAccountReplicationPolicy 2673
Utilização desta política 2673
Detalhes desta política 2673
Versão da política 2673
Documento da política JSON 2673
Saiba mais 2674
AWSElasticDisasterRecoveryEc2InstancePolicy 2674
Utilização desta política 2675
Detalhes desta política 2675
Versão da política 2675
Documento da política JSON 2675
Saiba mais 2677

AWSElasticDisasterRecoveryFailbackInstallationPolicy 2677
Utilização desta política 2678
Detalhes desta política 2678
Versão da política 2678
Documento da política JSON 2678
Saiba mais 2679
AWSElasticDisasterRecoveryFailbackPolicy 2679
Utilização desta política 2679
Detalhes desta política 2679
Versão da política 2680
Documento da política JSON 2680
Saiba mais 2681
AWSElasticDisasterRecoveryLaunchActionsPolicy 2681
Utilização desta política 2682
Detalhes desta política 2682
Versão da política 2682
Documento da política JSON 2682
Saiba mais 2688
AWSElasticDisasterRecoveryNetworkReplicationPolicy 2688
Utilização desta política 2689
Detalhes desta política 2689
Versão da política 2689
Documento da política JSON 2689
Saiba mais 2690
AWSElasticDisasterRecoveryReadOnlyAccess 2690
Utilização desta política 2690
Detalhes desta política 2690
Versão da política 2691
Documento da política JSON 2691
Saiba mais 2693
AWSElasticDisasterRecoveryRecoveryInstancePolicy 2693
Utilização desta política 2694
Detalhes desta política 2694
Versão da política 2694
Documento da política JSON 2694
Saiba mais 2697

AWSElasticDisasterRecoveryReplicationServerPolicy 2697
Utilização desta política 2697
Detalhes desta política 2697
Versão da política 2698
Documento da política JSON 2698
Saiba mais 2700
AWSElasticDisasterRecoveryServiceRolePolicy 2700
Utilização desta política 2700
Detalhes desta política 2701
Versão da política 2701
Documento da política JSON 2701
Saiba mais 2711
AWSElasticDisasterRecoveryStagingAccountPolicy 2711
Utilização desta política 2711
Detalhes desta política 2711
Versão da política 2712
Documento da política JSON 2712
Saiba mais 2713
AWSElasticDisasterRecoveryStagingAccountPolicy_v2 2713
Utilização desta política 2713
Detalhes desta política 2713
Versão da política 2714
Documento da política JSON 2714
Saiba mais 2715
AWSElasticLoadBalancingClassicServiceRolePolicy 2715
Utilização desta política 2715
Detalhes desta política 2716
Versão da política 2716
Documento da política JSON 2716
Saiba mais 2717
AWSElasticLoadBalancingServiceRolePolicy 2717
Utilização desta política 2717
Detalhes desta política 2717
Versão da política 2718
Documento da política JSON 2718
Saiba mais 2719

AWSElementalMediaConnectCreateBridge 2719
Utilização desta política 2719
Detalhes desta política 2719
Versão da política 2720
Documento da política JSON 2720
Saiba mais 2720
AWSElementalMediaConnectCreateFlow 2720
Utilização desta política 2721
Detalhes desta política 2721
Versão da política 2721
Documento da política JSON 2721
Saiba mais 2722
AWSElementalMediaConnectDeleteBridge 2722
Utilização desta política 2722
Detalhes desta política 2723
Versão da política 2723
Documento da política JSON 2723
Saiba mais 2723
AWSElementalMediaConnectDeleteFlow 2724
Utilização desta política 2724
Detalhes desta política 2724
Versão da política 2724
Documento da política JSON 2724
Saiba mais 2725
AWSElementalMediaConnectFullAccess 2725
Utilização desta política 2725
Detalhes desta política 2726
Versão da política 2726
Documento da política JSON 2726
Saiba mais 2726
AWSElementalMediaConnectReadOnlyAccess 2727
Utilização desta política 2727
Detalhes desta política 2727
Versão da política 2727
Documento da política JSON 2727
Saiba mais 2728

AWSElementalMediaConvertFullAccess 2728
Utilização desta política 2728
Detalhes desta política 2728
Versão da política 2729
Documento da política JSON 2729
Saiba mais 2730
AWSElementalMediaConvertReadOnly 2730
Utilização desta política 2730
Detalhes desta política 2730
Versão da política 2730
Documento da política JSON 2730
Saiba mais 2731
AWSElementalMediaLiveFullAccess 2731
Utilização desta política 2731
Detalhes desta política 2731
Versão da política 2732
Documento da política JSON 2732
Saiba mais 2732
AWSElementalMediaLiveReadOnly 2732
Utilização desta política 2732
Detalhes desta política 2733
Versão da política 2733
Documento da política JSON 2733
Saiba mais 2733
AWSElementalMediaPackageFullAccess 2734
Utilização desta política 2734
Detalhes desta política 2734
Versão da política 2734
Documento da política JSON 2734
Saiba mais 2735
AWSElementalMediaPackageReadOnly 2735
Utilização desta política 2735
Detalhes desta política 2735
Versão da política 2735
Documento da política JSON 2735
Saiba mais 2736

AWSElementalMediaPackageV2FullAccess 2736
Utilização desta política 2736
Detalhes desta política 2736
Versão da política 2736
Documento da política JSON 2737
Saiba mais 2737
AWSElementalMediaPackageV2ReadOnly 2737
Utilização desta política 2737
Detalhes desta política 2737
Versão da política 2738
Documento da política JSON 2738
Saiba mais 2738
AWSElementalMediaStoreFullAccess 2738
Utilização desta política 2739
Detalhes desta política 2739
Versão da política 2739
Documento da política JSON 2739
Saiba mais 2740
AWSElementalMediaStoreReadOnly 2740
Utilização desta política 2740
Detalhes desta política 2740
Versão da política 2740
Documento da política JSON 2740
Saiba mais 2741
AWSElementalMediaTailorFullAccess 2741
Utilização desta política 2741
Detalhes desta política 2741
Versão da política 2742
Documento da política JSON 2742
Saiba mais 2742
AWSElementalMediaTailorReadOnly 2742
Utilização desta política 2742
Detalhes desta política 2743
Versão da política 2743
Documento da política JSON 2743
Saiba mais 2743

AWSEnhancedClassicNetworkingMangementPolicy 2744
Utilização desta política 2744
Detalhes desta política 2744
Versão da política 2744
Documento da política JSON 2744
Saiba mais 2745
AWSEntityResolutionConsoleFullAccess 2745
Utilização desta política 2745
Detalhes desta política 2745
Versão da política 2745
Documento da política JSON 2746
Saiba mais 2749
AWSEntityResolutionConsoleReadOnlyAccess 2749
Utilização desta política 2749
Detalhes desta política 2749
Versão da política 2749
Documento da política JSON 2750
Saiba mais 2750
AWSFaultInjectionSimulatorEC2Access 2750
Utilização desta política 2750
Detalhes desta política 2751
Versão da política 2751
Documento da política JSON 2751
Saiba mais 2753
AWSFaultInjectionSimulatorECSAccess 2753
Utilização desta política 2753
Detalhes desta política 2753
Versão da política 2753
Documento da política JSON 2754
Saiba mais 2756
AWSFaultInjectionSimulatorEKSAccess 2756
Utilização desta política 2756
Detalhes desta política 2756
Versão da política 2756
Documento da política JSON 2757
Saiba mais 2758

AWSFaultInjectionSimulatorNetworkAccess 2758
Utilização desta política 2758
Detalhes desta política 2758
Versão da política 2758
Documento da política JSON 2759
Saiba mais 2766
AWSFaultInjectionSimulatorRDSAccess 2766
Utilização desta política 2766
Detalhes desta política 2766
Versão da política 2766
Documento da política JSON 2767
Saiba mais 2768
AWSFaultInjectionSimulatorSSMAccess 2768
Utilização desta política 2768
Detalhes desta política 2768
Versão da política 2768
Documento da política JSON 2769
Saiba mais 2770
AWSFinSpaceServiceRolePolicy 2770
Utilização desta política 2770
Detalhes desta política 2770
Versão da política 2771
Documento da política JSON 2771
Saiba mais 2771
AWSFMAdminFullAccess 2772
Utilização desta política 2772
Detalhes desta política 2772
Versão da política 2772
Documento da política JSON 2772
Saiba mais 2774
AWSFMAdminReadOnlyAccess 2774
Utilização desta política 2774
Detalhes desta política 2774
Versão da política 2775
Documento da política JSON 2775
Saiba mais 2776

AWSFMMemberReadOnlyAccess 2777
Utilização desta política 2777
Detalhes desta política 2777
Versão da política 2777
Documento da política JSON 2777
Saiba mais 2778
AWSForWordPressPluginPolicy 2778
Utilização desta política 2778
Detalhes desta política 2778
Versão da política 2778
Documento da política JSON 2779
Saiba mais 2781
AWSGitSyncServiceRolePolicy 2781
Utilização desta política 2781
Detalhes desta política 2782
Versão da política 2782
Documento da política JSON 2782
Saiba mais 2783
AWSGlobalAcceleratorSLRPolicy 2783
Utilização desta política 2783
Detalhes desta política 2783
Versão da política 2783
Documento da política JSON 2783
Saiba mais 2785
AWSGlueConsoleFullAccess 2785
Utilização desta política 2785
Detalhes desta política 2785
Versão da política 2786
Documento da política JSON 2786
Saiba mais 2790
AWSGlueConsoleSageMakerNotebookFullAccess 2791
Utilização desta política 2791
Detalhes desta política 2791
Versão da política 2791
Documento da política JSON 2791
Saiba mais 2797

AwsGlueDataBrewFullAccessPolicy 2797
Utilização desta política 2797
Detalhes desta política 2797
Versão da política 2797
Documento da política JSON 2798
Saiba mais 2803
AWSGlueDataBrewServiceRole 2803
Utilização desta política 2803
Detalhes desta política 2803
Versão da política 2803
Documento da política JSON 2804
Saiba mais 2806
AWSGlueSchemaRegistryFullAccess 2807
Utilização desta política 2807
Detalhes desta política 2807
Versão da política 2807
Documento da política JSON 2807
Saiba mais 2808
AWSGlueSchemaRegistryReadonlyAccess 2809
Utilização desta política 2809
Detalhes desta política 2809
Versão da política 2809
Documento da política JSON 2809
Saiba mais 2810
AWSGlueServiceNotebookRole 2810
Utilização desta política 2810
Detalhes desta política 2810
Versão da política 2811
Documento da política JSON 2811
Saiba mais 2813
AWSGlueServiceRole 2813
Utilização desta política 2814
Detalhes desta política 2814
Versão da política 2814
Documento da política JSON 2814
Saiba mais 2816

AwsGlueSessionUserRestrictedNotebookPolicy 2817
Utilização desta política 2817
Detalhes desta política 2817
Versão da política 2817
Documento da política JSON 2817
Saiba mais 2820
AwsGlueSessionUserRestrictedNotebookServiceRole 2820
Utilização desta política 2821
Detalhes desta política 2821
Versão da política 2821
Documento da política JSON 2821
Saiba mais 2825
AwsGlueSessionUserRestrictedPolicy 2825
Utilização desta política 2825
Detalhes desta política 2825
Versão da política 2826
Documento da política JSON 2826
Saiba mais 2829
AwsGlueSessionUserRestrictedServiceRole 2829
Utilização desta política 2829
Detalhes desta política 2829
Versão da política 2829
Documento da política JSON 2830
Saiba mais 2834
AWSGrafanaAccountAdministrator 2834
Utilização desta política 2834
Detalhes desta política 2834
Versão da política 2835
Documento da política JSON 2835
Saiba mais 2836
AWSGrafanaConsoleReadOnlyAccess 2836
Utilização desta política 2836
Detalhes desta política 2836
Versão da política 2836
Documento da política JSON 2837
Saiba mais 2837

AWSGrafanaWorkspacePermissionManagement 2837
Utilização desta política 2837
Detalhes desta política 2838
Versão da política 2838
Documento da política JSON 2838
Saiba mais 2839
AWSGrafanaWorkspacePermissionManagementV2 2839
Utilização desta política 2839
Detalhes desta política 2839
Versão da política 2840
Documento da política JSON 2840
Saiba mais 2841
AWSGreengrassFullAccess 2841
Utilização desta política 2841
Detalhes desta política 2841
Versão da política 2841
Documento da política JSON 2842
Saiba mais 2842
AWSGreengrassReadOnlyAccess 2842
Utilização desta política 2842
Detalhes desta política 2842
Versão da política 2843
Documento da política JSON 2843
Saiba mais 2843
AWSGreengrassResourceAccessRolePolicy 2843
Utilização desta política 2844
Detalhes desta política 2844
Versão da política 2844
Documento da política JSON 2844
Saiba mais 2846
AWSGroundStationAgentInstancePolicy 2847
Utilização desta política 2847
Detalhes desta política 2847
Versão da política 2847
Documento da política JSON 2847
Saiba mais 2848

AWSHealth_EventProcessorServiceRolePolicy 2848
Utilização desta política 2848
Detalhes desta política 2848
Versão da política 2848
Documento da política JSON 2849
Saiba mais 2849
AWSHealthFullAccess 2850
Utilização desta política 2850
Detalhes desta política 2850
Versão da política 2850
Documento da política JSON 2850
Saiba mais 2851
AWSHealthImagingFullAccess 2851
Utilização desta política 2852
Detalhes desta política 2852
Versão da política 2852
Documento da política JSON 2852
Saiba mais 2853
AWSHealthImagingReadOnlyAccess 2853
Utilização desta política 2853
Detalhes desta política 2853
Versão da política 2853
Documento da política JSON 2854
Saiba mais 2854
AWSHealthImagingServiceRolePolicy 2854
Utilização desta política 2855
Detalhes desta política 2855
Versão da política 2855
Documento da política JSON 2855
Saiba mais 2856
AWSHealthOmicsServiceLinkedRolePolicy 2856
Utilização desta política 2856
Detalhes desta política 2856
Versão da política 2856
Documento da política JSON 2857
Saiba mais 2859

AWSIAMIdentityCenterAllowListForIdentityContext 2859
Utilização desta política 2859
Detalhes desta política 2859
Versão da política 2859
Documento da política JSON 2859
Saiba mais 2863
AWSIAMRoleManagerServiceRolePolicy 2863
Utilização desta política 2863
Detalhes desta política 2863
Versão da política 2863
Documento da política JSON 2864
Saiba mais 2864
AWSIdentityCenterExternalManagementPolicy 2864
Utilização desta política 2865
Detalhes desta política 2865
Versão da política 2865
Documento da política JSON 2865
Saiba mais 2867
AWSIdentitySyncFullAccess 2867
Utilização desta política 2867
Detalhes desta política 2867
Versão da política 2867
Documento da política JSON 2868
Saiba mais 2868
AWSIdentitySyncReadOnlyAccess 2869
Utilização desta política 2869
Detalhes desta política 2869
Versão da política 2869
Documento da política JSON 2869
Saiba mais 2870
AWSImageBuilderFullAccess 2870
Utilização desta política 2870
Detalhes desta política 2870
Versão da política 2870
Documento da política JSON 2871
Saiba mais 2873

AWSImageBuilderReadOnlyAccess 2874
Utilização desta política 2874
Detalhes desta política 2874
Versão da política 2874
Documento da política JSON 2874
Saiba mais 2875
AWSImportExportFullAccess 2875
Utilização desta política 2875
Detalhes desta política 2875
Versão da política 2875
Documento da política JSON 2876
Saiba mais 2876
AWSImportExportReadOnlyAccess 2876
Utilização desta política 2876
Detalhes desta política 2876
Versão da política 2877
Documento da política JSON 2877
Saiba mais 2877
AWSIncidentManagerIncidentAccessServiceRolePolicy 2878
Utilização desta política 2878
Detalhes desta política 2878
Versão da política 2878
Documento da política JSON 2878
Saiba mais 2879
AWSIncidentManagerResolverAccess 2879
Utilização desta política 2879
Detalhes desta política 2879
Versão da política 2880
Documento da política JSON 2880
Saiba mais 2881
AWSIncidentManagerServiceRolePolicy 2881
Utilização desta política 2881
Detalhes desta política 2881
Versão da política 2882
Documento da política JSON 2882
Saiba mais 2883

AWSIoT1ClickFullAccess 2883
Utilização desta política 2883
Detalhes desta política 2883
Versão da política 2883
Documento da política JSON 2884
Saiba mais 2884
AWSIoT1ClickReadOnlyAccess 2884
Utilização desta política 2884
Detalhes desta política 2884
Versão da política 2885
Documento da política JSON 2885
Saiba mais 2885
AWSIoTAnalyticsFullAccess 2886
Utilização desta política 2886
Detalhes desta política 2886
Versão da política 2886
Documento da política JSON 2886
Saiba mais 2887
AWSIoTAnalyticsReadOnlyAccess 2887
Utilização desta política 2887
Detalhes desta política 2887
Versão da política 2887
Documento da política JSON 2887
Saiba mais 2888
AWSIoTConfigAccess 2888
Utilização desta política 2888
Detalhes desta política 2888
Versão da política 2889
Documento da política JSON 2889
Saiba mais 2893
AWSIoTConfigReadOnlyAccess 2893
Utilização desta política 2893
Detalhes desta política 2893
Versão da política 2893
Documento da política JSON 2893
Saiba mais 2895

AWSIoTDataAccess 2896
Utilização desta política 2896
Detalhes desta política 2896
Versão da política 2896
Documento da política JSON 2896
Saiba mais 2897
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction 2897
Utilização desta política 2897
Detalhes desta política 2897
Versão da política 2898
Documento da política JSON 2898
Saiba mais 2898
AWSIoTDeviceDefenderAudit 2898
Utilização desta política 2899
Detalhes desta política 2899
Versão da política 2899
Documento da política JSON 2899
Saiba mais 2900
AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction 2900
Utilização desta política 2900
Detalhes desta política 2900
Versão da política 2901
Documento da política JSON 2901
Saiba mais 2902
AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction 2902
Utilização desta política 2902
Detalhes desta política 2902
Versão da política 2902
Documento da política JSON 2903
Saiba mais 2903
AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction 2903
Utilização desta política 2904
Detalhes desta política 2904
Versão da política 2904
Documento da política JSON 2904
Saiba mais 2905

AWSIoTDeviceDefenderUpdateCACertMitigationAction 2905
Utilização desta política 2905
Detalhes desta política 2905
Versão da política 2905
Documento da política JSON 2906
Saiba mais 2906
AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction 2906
Utilização desta política 2906
Detalhes desta política 2907
Versão da política 2907
Documento da política JSON 2907
Saiba mais 2907
AWSIoTDeviceTesterForFreeRTOSFullAccess 2908
Utilização desta política 2908
Detalhes desta política 2908
Versão da política 2908
Documento da política JSON 2908
Saiba mais 2914
AWSIoTDeviceTesterForGreengrassFullAccess 2915
Utilização desta política 2915
Detalhes desta política 2915
Versão da política 2915
Documento da política JSON 2915
Saiba mais 2918
AWSIoTEventsFullAccess 2918
Utilização desta política 2919
Detalhes desta política 2919
Versão da política 2919
Documento da política JSON 2919
Saiba mais 2919
AWSIoTEventsReadOnlyAccess 2920
Utilização desta política 2920
Detalhes desta política 2920
Versão da política 2920
Documento da política JSON 2920
Saiba mais 2921

AWSIoTFleetHubFederationAccess 2921
Utilização desta política 2921
Detalhes desta política 2921
Versão da política 2921
Documento da política JSON 2922
Saiba mais 2923
AWSIoTFleetwiseServiceRolePolicy 2924
Utilização desta política 2924
Detalhes desta política 2924
Versão da política 2924
Documento da política JSON 2924
Saiba mais 2925
AWSIoTFullAccess 2925
Utilização desta política 2925
Detalhes desta política 2925
Versão da política 2925
Documento da política JSON 2926
Saiba mais 2926
AWSIoTLogging 2926
Utilização desta política 2926
Detalhes desta política 2927
Versão da política 2927
Documento da política JSON 2927
Saiba mais 2928
AWSIoTManagedIntegrationsFullAccess 2928
Utilização desta política 2928
Detalhes desta política 2928
Versão da política 2928
Documento da política JSON 2928
Saiba mais 2929
AWSIoTManagedIntegrationsRolePolicy 2929
Utilização desta política 2929
Detalhes desta política 2930
Versão da política 2930
Documento da política JSON 2930
Saiba mais 2931

AWSIoTOTAUpdate 2931
Utilização desta política 2932
Detalhes desta política 2932
Versão da política 2932
Documento da política JSON 2932
Saiba mais 2932
AWSIotRoboRunnerFullAccess 2933
Utilização desta política 2933
Detalhes desta política 2933
Versão da política 2933
Documento da política JSON 2933
Saiba mais 2934
AWSIotRoboRunnerReadOnly 2934
Utilização desta política 2934
Detalhes desta política 2934
Versão da política 2935
Documento da política JSON 2935
Saiba mais 2935
AWSIotRoboRunnerServiceRolePolicy 2936
Utilização desta política 2936
Detalhes desta política 2936
Versão da política 2936
Documento da política JSON 2936
Saiba mais 2937
AWSIoTRuleActions 2937
Utilização desta política 2937
Detalhes desta política 2937
Versão da política 2937
Documento da política JSON 2938
Saiba mais 2938
AWSIoTSiteWiseConsoleFullAccess 2938
Utilização desta política 2939
Detalhes desta política 2939
Versão da política 2939
Documento da política JSON 2939
Saiba mais 2941

AWSIoTSiteWiseFullAccess 2941
Utilização desta política 2941
Detalhes desta política 2942
Versão da política 2942
Documento da política JSON 2942
Saiba mais 2942
AWSIoTSiteWiseMonitorPortalAccess 2943
Utilização desta política 2943
Detalhes desta política 2943
Versão da política 2943
Documento da política JSON 2943
Saiba mais 2944
AWSIoTSiteWiseMonitorServiceRolePolicy 2945
Utilização desta política 2945
Detalhes desta política 2945
Versão da política 2945
Documento da política JSON 2945
Saiba mais 2946
AWSIoTSiteWiseReadOnlyAccess 2946
Utilização desta política 2947
Detalhes desta política 2947
Versão da política 2947
Documento da política JSON 2947
Saiba mais 2949
AWSIoTThingsRegistration 2949
Utilização desta política 2949
Detalhes desta política 2949
Versão da política 2949
Documento da política JSON 2950
Saiba mais 2951
AWSIoTTwinMakerServiceRolePolicy 2951
Utilização desta política 2951
Detalhes desta política 2951
Versão da política 2951
Documento da política JSON 2952
Saiba mais 2953

AWSIoTWirelessDataAccess 2953
Utilização desta política 2953
Detalhes desta política 2954
Versão da política 2954
Documento da política JSON 2954
Saiba mais 2954
AWSIoTWirelessFullAccess 2955
Utilização desta política 2955
Detalhes desta política 2955
Versão da política 2955
Documento da política JSON 2955
Saiba mais 2956
AWSIoTWirelessFullPublishAccess 2956
Utilização desta política 2956
Detalhes desta política 2956
Versão da política 2956
Documento da política JSON 2956
Saiba mais 2957
AWSIoTWirelessGatewayCertManager 2957
Utilização desta política 2957
Detalhes desta política 2957
Versão da política 2958
Documento da política JSON 2958
Saiba mais 2958
AWSIoTWirelessLogging 2958
Utilização desta política 2959
Detalhes desta política 2959
Versão da política 2959
Documento da política JSON 2959
Saiba mais 2960
AWSIoTWirelessReadOnlyAccess 2960
Utilização desta política 2960
Detalhes desta política 2960
Versão da política 2960
Documento da política JSON 2960
Saiba mais 2961

AWSIPAMServiceRolePolicy 2961
Utilização desta política 2961
Detalhes desta política 2961
Versão da política 2962
Documento da política JSON 2962
Saiba mais 2964
AWSIQContractServiceRolePolicy 2964
Utilização desta política 2964
Detalhes desta política 2964
Versão da política 2964
Documento da política JSON 2965
Saiba mais 2965
AWSIQFullAccess 2965
Utilização desta política 2965
Detalhes desta política 2965
Versão da política 2966
Documento da política JSON 2966
Saiba mais 2966
AWSIQPermissionServiceRolePolicy 2967
Utilização desta política 2967
Detalhes desta política 2967
Versão da política 2967
Documento da política JSON 2967
Saiba mais 2968
AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy 2968
Utilização desta política 2969
Detalhes desta política 2969
Versão da política 2969
Documento da política JSON 2969
Saiba mais 2970
AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy 2970
Utilização desta política 2970
Detalhes desta política 2970
Versão da política 2970
Documento da política JSON 2971
Saiba mais 2971

AWSKeyManagementServicePowerUser 2971
Utilização desta política 2971
Detalhes desta política 2971
Versão da política 2972
Documento da política JSON 2972
Saiba mais 2972
AWSLakeFormationCrossAccountManager 2973
Utilização desta política 2973
Detalhes desta política 2973
Versão da política 2973
Documento da política JSON 2973
Saiba mais 2975
AWSLakeFormationDataAdmin 2976
Utilização desta política 2976
Detalhes desta política 2976
Versão da política 2976
Documento da política JSON 2976
Saiba mais 2978
AWSLambda_FullAccess 2978
Utilização desta política 2978
Detalhes desta política 2978
Versão da política 2978
Documento da política JSON 2979
Saiba mais 2980
AWSLambda_ReadOnlyAccess 2980
Utilização desta política 2981
Detalhes desta política 2981
Versão da política 2981
Documento da política JSON 2981
Saiba mais 2982
AWSLambdaBasicDurableExecutionRolePolicy 2983
Utilização desta política 2983
Detalhes desta política 2983
Versão da política 2983
Documento da política JSON 2983
Saiba mais 2984

AWSLambdaBasicExecutionRole 2984
Utilização desta política 2984
Detalhes desta política 2984
Versão da política 2984
Documento da política JSON 2985
Saiba mais 2985
AWSLambdaDynamoDBExecutionRole 2985
Utilização desta política 2985
Detalhes desta política 2986
Versão da política 2986
Documento da política JSON 2986
Saiba mais 2986
AWSLambdaENIManagementAccess 2987
Utilização desta política 2987
Detalhes desta política 2987
Versão da política 2987
Documento da política JSON 2987
Saiba mais 2988
AWSLambdaExecute 2988
Utilização desta política 2988
Detalhes desta política 2989
Versão da política 2989
Documento da política JSON 2989
Saiba mais 2990
AWSLambdaFullAccess 2990
Utilização desta política 2990
Detalhes desta política 2990
Versão da política 2990
Documento da política JSON 2990
Saiba mais 2992
AWSLambdaInvocation-DynamoDB 2992
Utilização desta política 2992
Detalhes desta política 2992
Versão da política 2993
Documento da política JSON 2993
Saiba mais 2993

AWSLambdaInvokeWebFunctionEndpointAccess 2994
Utilização desta política 2994
Detalhes desta política 2994
Versão da política 2994
Documento da política JSON 2994
Saiba mais 2995
AWSLambdaKinesisExecutionRole 2995
Utilização desta política 2995
Detalhes desta política 2995
Versão da política 2995
Documento da política JSON 2996
Saiba mais 2996
AWSLambdaManagedEC2ResourceOperator 2996
Utilização desta política 2997
Detalhes desta política 2997
Versão da política 2997
Documento da política JSON 2997
Saiba mais 2999
AWSLambdaMSKExecutionRole 2999
Utilização desta política 2999
Detalhes desta política 2999
Versão da política 3000
Documento da política JSON 3000
Saiba mais 3001
AWSLambdaNetworkConnectorOperatorPolicy 3001
Utilização desta política 3001
Detalhes desta política 3001
Versão da política 3001
Documento da política JSON 3001
Saiba mais 3003
AWSLambdaReplicator 3003
Utilização desta política 3003
Detalhes desta política 3003
Versão da política 3003
Documento da política JSON 3004
Saiba mais 3005

AWSLambdaRole 3005
Utilização desta política 3005
Detalhes desta política 3005
Versão da política 3005
Documento da política JSON 3005
Saiba mais 3006
AWSLambdaServiceRolePolicy 3006
Utilização desta política 3006
Detalhes desta política 3006
Versão da política 3007
Documento da política JSON 3007
Saiba mais 3008
AWSLambdaSQSQueueExecutionRole 3008
Utilização desta política 3008
Detalhes desta política 3008
Versão da política 3009
Documento da política JSON 3009
Saiba mais 3009
AWSLambdaVPCAccessExecutionRole 3010
Utilização desta política 3010
Detalhes desta política 3010
Versão da política 3010
Documento da política JSON 3010
Saiba mais 3011
AWSLicenseManagerConsumptionPolicy 3011
Utilização desta política 3011
Detalhes desta política 3011
Versão da política 3012
Documento da política JSON 3012
Saiba mais 3012
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy 3012
Utilização desta política 3013
Detalhes desta política 3013
Versão da política 3013
Documento da política JSON 3013
Saiba mais 3015

AWSLicenseManagerMasterAccountRolePolicy 3015
Utilização desta política 3015
Detalhes desta política 3015
Versão da política 3016
Documento da política JSON 3016
Saiba mais 3021
AWSLicenseManagerMemberAccountRolePolicy 3021
Utilização desta política 3021
Detalhes desta política 3021
Versão da política 3021
Documento da política JSON 3021
Saiba mais 3023
AWSLicenseManagerServiceRolePolicy 3023
Utilização desta política 3023
Detalhes desta política 3023
Versão da política 3023
Documento da política JSON 3023
Saiba mais 3027
AWSLicenseManagerUserSubscriptionsServiceRolePolicy 3027
Utilização desta política 3027
Detalhes desta política 3027
Versão da política 3028
Documento da política JSON 3028
Saiba mais 3031
AWSM2ServicePolicy 3031
Utilização desta política 3031
Detalhes desta política 3031
Versão da política 3032
Documento da política JSON 3032
Saiba mais 3033
AWSManagedAccountManagementAccess 3033
Utilização desta política 3033
Detalhes desta política 3034
Versão da política 3034
Documento da política JSON 3034
Saiba mais 3035

AWSManagedAccountUserEntitlementAccess 3035
Utilização desta política 3035
Detalhes desta política 3035
Versão da política 3036
Documento da política JSON 3036
Saiba mais 3036
AWSManagedAdvancedFeaturesActivationAccess 3036
Utilização desta política 3037
Detalhes desta política 3037
Versão da política 3037
Documento da política JSON 3037
Saiba mais 3037
AWSManagedBudgetsSpendLimitManagementAccess 3038
Utilização desta política 3038
Detalhes desta política 3038
Versão da política 3038
Documento da política JSON 3038
Saiba mais 3039
AWSManagedControlPolicyManagementAccess 3040
Utilização desta política 3040
Detalhes desta política 3040
Versão da política 3040
Documento da política JSON 3040
Saiba mais 3041
AWSManagedServiceAccessManagementAccess 3041
Utilização desta política 3041
Detalhes desta política 3041
Versão da política 3042
Documento da política JSON 3042
Saiba mais 3044
AWSManagedServices_ContactsServiceRolePolicy 3044
Utilização desta política 3044
Detalhes desta política 3044
Versão da política 3044
Documento da política JSON 3045
Saiba mais 3045

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy 3045
Utilização desta política 3046
Detalhes desta política 3046
Versão da política 3046
Documento da política JSON 3046
Saiba mais 3048
AWSManagedServices_EventsServiceRolePolicy 3048
Utilização desta política 3048
Detalhes desta política 3048
Versão da política 3048
Documento da política JSON 3049
Saiba mais 3049
AWSManagedServices_SelfServiceReporting_ServiceRolePolicy 3050
Utilização desta política 3050
Detalhes desta política 3050
Versão da política 3050
Documento da política JSON 3050
Saiba mais 3051
AWSManagedServicesDeploymentToolkitPolicy 3051
Utilização desta política 3051
Detalhes desta política 3051
Versão da política 3052
Documento da política JSON 3052
Saiba mais 3054
AWSManagedSettingsAdminAccess 3054
Utilização desta política 3054
Detalhes desta política 3054
Versão da política 3055
Documento da política JSON 3055
Saiba mais 3065
AWSManagedSettingsReadOnlyAccess 3065
Utilização desta política 3065
Detalhes desta política 3066
Versão da política 3066
Documento da política JSON 3066
Saiba mais 3067

AWSManagedSignUpAdminAccess 3068
Utilização desta política 3068
Detalhes desta política 3068
Versão da política 3068
Documento da política JSON 3068
Saiba mais 3070
AWSManagementConsoleAdministratorAccess 3070
Utilização desta política 3070
Detalhes desta política 3070
Versão da política 3071
Documento da política JSON 3071
Saiba mais 3073
AWSManagementConsoleBasicUserAccess 3073
Utilização desta política 3074
Detalhes desta política 3074
Versão da política 3074
Documento da política JSON 3074
Saiba mais 3075
AWSMarketplaceAmiIngestion 3075
Utilização desta política 3076
Detalhes desta política 3076
Versão da política 3076
Documento da política JSON 3076
Saiba mais 3077
AWSMarketplaceDeploymentServiceRolePolicy 3077
Utilização desta política 3077
Detalhes desta política 3077
Versão da política 3077
Documento da política JSON 3078
Saiba mais 3079
AWSMarketplaceDiscoveryFullAccess 3079
Utilização desta política 3079
Detalhes desta política 3079
Versão da política 3080
Documento da política JSON 3080
Saiba mais 3081

AWSMarketplaceFullAccess 3081
Utilização desta política 3081
Detalhes desta política 3081
Versão da política 3081
Documento da política JSON 3081
Saiba mais 3084
AWSMarketplaceGetEntitlements 3084
Utilização desta política 3084
Detalhes desta política 3084
Versão da política 3085
Documento da política JSON 3085
Saiba mais 3085
AWSMarketplaceImageBuildFullAccess 3085
Utilização desta política 3086
Detalhes desta política 3086
Versão da política 3086
Documento da política JSON 3086
Saiba mais 3090
AWSMarketplaceLicenseManagementServiceRolePolicy 3090
Utilização desta política 3090
Detalhes desta política 3090
Versão da política 3090
Documento da política JSON 3091
Saiba mais 3091
AWSMarketplaceManageSubscriptions 3091
Utilização desta política 3091
Detalhes desta política 3092
Versão da política 3092
Documento da política JSON 3092
Saiba mais 3095
AWSMarketplaceMeteringFullAccess 3095
Utilização desta política 3095
Detalhes desta política 3096
Versão da política 3096
Documento da política JSON 3096
Saiba mais 3096

AWSMarketplaceMeteringRegisterUsage 3097
Utilização desta política 3097
Detalhes desta política 3097
Versão da política 3097
Documento da política JSON 3097
Saiba mais 3098
AWSMarketplaceProcurementSystemAdminFullAccess 3098
Utilização desta política 3098
Detalhes desta política 3098
Versão da política 3098
Documento da política JSON 3099
Saiba mais 3099
AWSMarketplacePurchaseOrdersServiceRolePolicy 3099
Utilização desta política 3100
Detalhes desta política 3100
Versão da política 3100
Documento da política JSON 3100
Saiba mais 3101
AWSMarketplaceRead-only 3101
Utilização desta política 3101
Detalhes desta política 3101
Versão da política 3101
Documento da política JSON 3101
Saiba mais 3103
AWSMarketplaceResaleAuthorizationServiceRolePolicy 3104
Utilização desta política 3104
Detalhes desta política 3104
Versão da política 3104
Documento da política JSON 3104
Saiba mais 3107
AWSMarketplaceSellerFullAccess 3107
Utilização desta política 3107
Detalhes desta política 3107
Versão da política 3107
Documento da política JSON 3107
Saiba mais 3114

AWSMarketplaceSellerOfferManagement 3115
Utilização desta política 3115
Detalhes desta política 3115
Versão da política 3115
Documento da política JSON 3115
Saiba mais 3118
AWSMarketplaceSellerProductsFullAccess 3118
Utilização desta política 3118
Detalhes desta política 3118
Versão da política 3119
Documento da política JSON 3119
Saiba mais 3122
AWSMarketplaceSellerProductsReadOnly 3122
Utilização desta política 3122
Detalhes desta política 3122
Versão da política 3123
Documento da política JSON 3123
Saiba mais 3124
AWSMcpServiceActionsFullAccess 3124
Utilização desta política 3124
Detalhes desta política 3124
Versão da política 3124
Documento da política JSON 3125
Saiba mais 3125
AWSMCPSignInOAuthAccessPolicy 3125
Utilização desta política 3125
Detalhes desta política 3125
Versão da política 3126
Documento da política JSON 3126
Saiba mais 3126
AWSMediaConnectServicePolicy 3127
Utilização desta política 3127
Detalhes desta política 3127
Versão da política 3127
Documento da política JSON 3127
Saiba mais 3129

AWSMediaLiveAnywhereServiceRolePolicy 3129
Utilização desta política 3129
Detalhes desta política 3130
Versão da política 3130
Documento da política JSON 3130
Saiba mais 3133
AWSMediaTailorServiceRolePolicy 3133
Utilização desta política 3133
Detalhes desta política 3133
Versão da política 3134
Documento da política JSON 3134
Saiba mais 3134
AWSMigrationHubDiscoveryAccess 3134
Utilização desta política 3135
Detalhes desta política 3135
Versão da política 3135
Documento da política JSON 3135
Saiba mais 3136
AWSMigrationHubDMSAccess 3137
Utilização desta política 3137
Detalhes desta política 3137
Versão da política 3137
Documento da política JSON 3137
Saiba mais 3138
AWSMigrationHubFullAccess 3138
Utilização desta política 3139
Detalhes desta política 3139
Versão da política 3139
Documento da política JSON 3139
Saiba mais 3140
AWSMigrationHubOrchestratorConsoleFullAccess 3141
Utilização desta política 3141
Detalhes desta política 3141
Versão da política 3141
Documento da política JSON 3141
Saiba mais 3144

AWSMigrationHubOrchestratorInstanceRolePolicy 3145
Utilização desta política 3145
Detalhes desta política 3145
Versão da política 3145
Documento da política JSON 3145
Saiba mais 3146
AWSMigrationHubOrchestratorPlugin 3146
Utilização desta política 3146
Detalhes desta política 3146
Versão da política 3147
Documento da política JSON 3147
Saiba mais 3148
AWSMigrationHubOrchestratorServiceRolePolicy 3148
Utilização desta política 3148
Detalhes desta política 3149
Versão da política 3149
Documento da política JSON 3149
Saiba mais 3152
AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess 3153
Utilização desta política 3153
Detalhes desta política 3153
Versão da política 3153
Documento da política JSON 3153
Saiba mais 3159
AWSMigrationHubRefactorSpaces-SSMAutomationPolicy 3159
Utilização desta política 3159
Detalhes desta política 3160
Versão da política 3160
Documento da política JSON 3160
Saiba mais 3161
AWSMigrationHubRefactorSpacesFullAccess 3162
Utilização desta política 3162
Detalhes desta política 3162
Versão da política 3162
Documento da política JSON 3162
Saiba mais 3169

AWSMigrationHubRefactorSpacesServiceRolePolicy 3169
Utilização desta política 3169
Detalhes desta política 3169
Versão da política 3170
Documento da política JSON 3170
Saiba mais 3173
AWSMigrationHubSMSAccess 3174
Utilização desta política 3174
Detalhes desta política 3174
Versão da política 3174
Documento da política JSON 3174
Saiba mais 3175
AWSMigrationHubStrategyCollector 3175
Utilização desta política 3176
Detalhes desta política 3176
Versão da política 3176
Documento da política JSON 3176
Saiba mais 3178
AWSMigrationHubStrategyConsoleFullAccess 3179
Utilização desta política 3179
Detalhes desta política 3179
Versão da política 3179
Documento da política JSON 3179
Saiba mais 3181
AWSMigrationHubStrategyServiceRolePolicy 3181
Utilização desta política 3181
Detalhes desta política 3181
Versão da política 3182
Documento da política JSON 3182
Saiba mais 3183
AWSMobileHub_FullAccess 3183
Utilização desta política 3183
Detalhes desta política 3183
Versão da política 3183
Documento da política JSON 3184
Saiba mais 3185

AWSMobileHub_ReadOnly 3185
Utilização desta política 3186
Detalhes desta política 3186
Versão da política 3186
Documento da política JSON 3186
Saiba mais 3187
AWSMSKReplicatorExecutionRole 3187
Utilização desta política 3188
Detalhes desta política 3188
Versão da política 3188
Documento da política JSON 3188
Saiba mais 3189
AWSNATGatewayServiceRolePolicy 3190
Utilização desta política 3190
Detalhes desta política 3190
Versão da política 3190
Documento da política JSON 3190
Saiba mais 3191
AWSNetworkFirewallFullAccess 3191
Utilização desta política 3191
Detalhes desta política 3191
Versão da política 3192
Documento da política JSON 3192
Saiba mais 3196
AWSNetworkFirewallReadOnlyAccess 3196
Utilização desta política 3196
Detalhes desta política 3196
Versão da política 3196
Documento da política JSON 3197
Saiba mais 3198
AWSNetworkFirewallServiceRolePolicy 3198
Utilização desta política 3198
Detalhes desta política 3198
Versão da política 3198
Documento da política JSON 3199
Saiba mais 3200

AWSNetworkManagerCloudWANServiceRolePolicy 3201
Utilização desta política 3201
Detalhes desta política 3201
Versão da política 3201
Documento da política JSON 3201
Saiba mais 3202
AWSNetworkManagerFullAccess 3202
Utilização desta política 3202
Detalhes desta política 3202
Versão da política 3202
Documento da política JSON 3203
Saiba mais 3203
AWSNetworkManagerReadOnlyAccess 3204
Utilização desta política 3204
Detalhes desta política 3204
Versão da política 3204
Documento da política JSON 3204
Saiba mais 3205
AWSNetworkManagerServiceRolePolicy 3205
Utilização desta política 3205
Detalhes desta política 3205
Versão da política 3205
Documento da política JSON 3206
Saiba mais 3207
AWSObservabilityAdminLogsCentralizationServiceRolePolicy 3207
Utilização desta política 3207
Detalhes desta política 3207
Versão da política 3207
Documento da política JSON 3208
Saiba mais 3208
AWSObservabilityAdminServiceRolePolicy 3209
Utilização desta política 3209
Detalhes desta política 3209
Versão da política 3209
Documento da política JSON 3209
Saiba mais 3212

AWSObservabilityAdminTelemetryEnablementServiceRolePolicy 3212
Utilização desta política 3212
Detalhes desta política 3212
Versão da política 3213
Documento da política JSON 3213
Saiba mais 3230
AWSOrganizationsFullAccess 3230
Utilização desta política 3230
Detalhes desta política 3231
Versão da política 3231
Documento da política JSON 3231
Saiba mais 3232
AWSOrganizationsReadOnlyAccess 3232
Utilização desta política 3232
Detalhes desta política 3232
Versão da política 3233
Documento da política JSON 3233
Saiba mais 3234
AWSOrganizationsServiceTrustPolicy 3234
Utilização desta política 3234
Detalhes desta política 3234
Versão da política 3234
Documento da política JSON 3235
Saiba mais 3235
AWSOutpostsAuthorizeServerPolicy 3235
Utilização desta política 3236
Detalhes desta política 3236
Versão da política 3236
Documento da política JSON 3236
Saiba mais 3236
AWSOutpostsServiceRolePolicy 3237
Utilização desta política 3237
Detalhes desta política 3237
Versão da política 3237
Documento da política JSON 3237
Saiba mais 3239

AWSPanoramaApplianceRolePolicy 3239
Utilização desta política 3239
Detalhes desta política 3240
Versão da política 3240
Documento da política JSON 3240
Saiba mais 3241
AWSPanoramaApplianceServiceRolePolicy 3241
Utilização desta política 3241
Detalhes desta política 3241
Versão da política 3241
Documento da política JSON 3242
Saiba mais 3243
AWSPanoramaFullAccess 3243
Utilização desta política 3243
Detalhes desta política 3243
Versão da política 3244
Documento da política JSON 3244
Saiba mais 3246
AWSPanoramaGreengrassGroupRolePolicy 3247
Utilização desta política 3247
Detalhes desta política 3247
Versão da política 3247
Documento da política JSON 3247
Saiba mais 3249
AWSPanoramaSageMakerRolePolicy 3249
Utilização desta política 3249
Detalhes desta política 3249
Versão da política 3249
Documento da política JSON 3250
Saiba mais 3250
AWSPanoramaServiceLinkedRolePolicy 3250
Utilização desta política 3250
Detalhes desta política 3251
Versão da política 3251
Documento da política JSON 3251
Saiba mais 3254

AWSPanoramaServiceRolePolicy 3254
Utilização desta política 3254
Detalhes desta política 3254
Versão da política 3254
Documento da política JSON 3254
Saiba mais 3261
AWSPartnerCentralChannelHandshakeApprovalManagement 3262
Utilização desta política 3262
Detalhes desta política 3262
Versão da política 3262
Documento da política JSON 3262
Saiba mais 3263
AWSPartnerCentralChannelManagement 3263
Utilização desta política 3263
Detalhes desta política 3263
Versão da política 3264
Documento da política JSON 3264
Saiba mais 3267
AWSPartnerCentralFullAccess 3267
Utilização desta política 3267
Detalhes desta política 3267
Versão da política 3267
Documento da política JSON 3267
Saiba mais 3272
AWSPartnerCentralMarketingManagement 3272
Utilização desta política 3272
Detalhes desta política 3272
Versão da política 3272
Documento da política JSON 3273
Saiba mais 3275
AWSPartnerCentralOpportunityManagement 3275
Utilização desta política 3276
Detalhes desta política 3276
Versão da política 3276
Documento da política JSON 3276
Saiba mais 3280

AWSPartnerCentralRevenueAttributionManagement 3281
Utilização desta política 3281
Detalhes desta política 3281
Versão da política 3281
Documento da política JSON 3281
Saiba mais 3286
AWSPartnerCentralSandboxFullAccess 3286
Utilização desta política 3286
Detalhes desta política 3286
Versão da política 3286
Documento da política JSON 3287
Saiba mais 3288
AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy 3288
Utilização desta política 3288
Detalhes desta política 3288
Versão da política 3289
Documento da política JSON 3289
Saiba mais 3290
AWSPartnerLedSupportReadOnlyAccess 3290
Utilização desta política 3290
Detalhes desta política 3290
Versão da política 3290
Documento da política JSON 3291
Saiba mais 3327
AWSPartnerProServeToolsFullAccess 3328
Utilização desta política 3328
Detalhes desta política 3328
Versão da política 3328
Documento da política JSON 3328
Saiba mais 3329
AWSPartnerProServeToolsIndividualContributor 3329
Utilização desta política 3329
Detalhes desta política 3329
Versão da política 3330
Documento da política JSON 3330
Saiba mais 3330

AWSPartnerProServeToolsOrganizationReaderIndividualContributor 3331
Utilização desta política 3331
Detalhes desta política 3331
Versão da política 3331
Documento da política JSON 3331
Saiba mais 3332
AWSPCSComputeNodePolicy 3332
Utilização desta política 3332
Detalhes desta política 3332
Versão da política 3333
Documento da política JSON 3333
Saiba mais 3333
AWSPCSServiceRolePolicy 3333
Utilização desta política 3334
Detalhes desta política 3334
Versão da política 3334
Documento da política JSON 3334
Saiba mais 3339
AWSPriceListServiceFullAccess 3339
Utilização desta política 3339
Detalhes desta política 3339
Versão da política 3340
Documento da política JSON 3340
Saiba mais 3340
AWSPrivateCAAuditor 3340
Utilização desta política 3341
Detalhes desta política 3341
Versão da política 3341
Documento da política JSON 3341
Saiba mais 3342
AWSPrivateCAConnectorForKubernetesPolicy 3342
Utilização desta política 3342
Detalhes desta política 3342
Versão da política 3343
Documento da política JSON 3343
Saiba mais 3343

AWSPrivateCAFullAccess 3343
Utilização desta política 3344
Detalhes desta política 3344
Versão da política 3344
Documento da política JSON 3344
Saiba mais 3344
AWSPrivateCAPrivilegedUser 3345
Utilização desta política 3345
Detalhes desta política 3345
Versão da política 3345
Documento da política JSON 3345
Saiba mais 3347
AWSPrivateCAReadOnly 3347
Utilização desta política 3347
Detalhes desta política 3347
Versão da política 3347
Documento da política JSON 3347
Saiba mais 3348
AWSPrivateCAUser 3348
Utilização desta política 3348
Detalhes desta política 3348
Versão da política 3349
Documento da política JSON 3349
Saiba mais 3350
AWSPrivateMarketplaceAdminFullAccess 3350
Utilização desta política 3350
Detalhes desta política 3350
Versão da política 3351
Documento da política JSON 3351
Saiba mais 3354
AWSPrivateMarketplaceRequests 3354
Utilização desta política 3354
Detalhes desta política 3354
Versão da política 3354
Documento da política JSON 3354
Saiba mais 3356

AWSPrivateNetworksServiceRolePolicy 3356
Utilização desta política 3357
Detalhes desta política 3357
Versão da política 3357
Documento da política JSON 3357
Saiba mais 3358
AWSProtonCodeBuildProvisioningBasicAccess 3358
Utilização desta política 3358
Detalhes desta política 3358
Versão da política 3358
Documento da política JSON 3358
Saiba mais 3359
AWSProtonCodeBuildProvisioningServiceRolePolicy 3359
Utilização desta política 3359
Detalhes desta política 3360
Versão da política 3360
Documento da política JSON 3360
Saiba mais 3361
AWSProtonDeveloperAccess 3361
Utilização desta política 3362
Detalhes desta política 3362
Versão da política 3362
Documento da política JSON 3362
Saiba mais 3364
AWSProtonFullAccess 3365
Utilização desta política 3365
Detalhes desta política 3365
Versão da política 3365
Documento da política JSON 3365
Saiba mais 3367
AWSProtonReadOnlyAccess 3368
Utilização desta política 3368
Detalhes desta política 3368
Versão da política 3368
Documento da política JSON 3368
Saiba mais 3370

AWSProtonServiceGitSyncServiceRolePolicy 3370
Utilização desta política 3370
Detalhes desta política 3370
Versão da política 3370
Documento da política JSON 3371
Saiba mais 3371
AWSProtonSyncServiceRolePolicy 3371
Utilização desta política 3372
Detalhes desta política 3372
Versão da política 3372
Documento da política JSON 3372
Saiba mais 3373
AWSPurchaseOrdersServiceRolePolicy 3373
Utilização desta política 3374
Detalhes desta política 3374
Versão da política 3374
Documento da política JSON 3374
Saiba mais 3375
AWSQuickSetupCFGCPacksPermissionsBoundary 3375
Utilização desta política 3375
Detalhes desta política 3375
Versão da política 3376
Documento da política JSON 3376
Saiba mais 3379
AWSQuickSetupDeploymentRolePolicy 3379
Utilização desta política 3379
Detalhes desta política 3379
Versão da política 3379
Documento da política JSON 3380
Saiba mais 3388
AWSQuickSetupDevOpsGuruPermissionsBoundary 3388
Utilização desta política 3389
Detalhes desta política 3389
Versão da política 3389
Documento da política JSON 3389
Saiba mais 3392

AWSQuickSetupDistributorPermissionsBoundary 3392
Utilização desta política 3392
Detalhes desta política 3392
Versão da política 3393
Documento da política JSON 3393
Saiba mais 3399
AWSQuickSetupEnableAREXExecutionPolicy 3399
Utilização desta política 3399
Detalhes desta política 3399
Versão da política 3399
Documento da política JSON 3400
Saiba mais 3401
AWSQuickSetupEnableDHMCExecutionPolicy 3401
Utilização desta política 3402
Detalhes desta política 3402
Versão da política 3402
Documento da política JSON 3402
Saiba mais 3403
AWSQuickSetupJITNADeploymentRolePolicy 3403
Utilização desta política 3404
Detalhes desta política 3404
Versão da política 3404
Documento da política JSON 3404
Saiba mais 3408
AWSQuickSetupManagedInstanceProfileExecutionPolicy 3408
Utilização desta política 3408
Detalhes desta política 3409
Versão da política 3409
Documento da política JSON 3409
Saiba mais 3414
AWSQuickSetupManageJITNAResourcesExecutionPolicy 3414
Utilização desta política 3414
Detalhes desta política 3414
Versão da política 3415
Documento da política JSON 3415
Saiba mais 3417

AWSQuickSetupPatchPolicyBaselineAccess 3417
Utilização desta política 3417
Detalhes desta política 3417
Versão da política 3418
Documento da política JSON 3418
Saiba mais 3419
AWSQuickSetupPatchPolicyDeploymentRolePolicy 3419
Utilização desta política 3419
Detalhes desta política 3419
Versão da política 3419
Documento da política JSON 3419
Saiba mais 3428
AWSQuickSetupPatchPolicyLambdaExecutionPolicy 3428
Utilização desta política 3428
Detalhes desta política 3428
Versão da política 3429
Documento da política JSON 3429
Saiba mais 3430
AWSQuickSetupPatchPolicyPermissionsBoundary 3430
Utilização desta política 3430
Detalhes desta política 3430
Versão da política 3430
Documento da política JSON 3431
Saiba mais 3439
AWSQuickSetupPatchPolicyTagManagementExecutionPolicy 3439
Utilização desta política 3439
Detalhes desta política 3439
Versão da política 3440
Documento da política JSON 3440
Saiba mais 3441
AWSQuickSetupSchedulerPermissionsBoundary 3441
Utilização desta política 3441
Detalhes desta política 3441
Versão da política 3442
Documento da política JSON 3442
Saiba mais 3445

AWSQuickSetupSSMDeploymentRolePolicy 3445
Utilização desta política 3445
Detalhes desta política 3446
Versão da política 3446
Documento da política JSON 3446
Saiba mais 3457
AWSQuickSetupSSMDeploymentS3BucketRolePolicy 3457
Utilização desta política 3457
Detalhes desta política 3458
Versão da política 3458
Documento da política JSON 3458
Saiba mais 3459
AWSQuickSetupSSMHostMgmtPermissionsBoundary 3459
Utilização desta política 3459
Detalhes desta política 3459
Versão da política 3459
Documento da política JSON 3460
Saiba mais 3465
AWSQuickSetupSSMLifecycleManagementExecutionPolicy 3466
Utilização desta política 3466
Detalhes desta política 3466
Versão da política 3466
Documento da política JSON 3466
Saiba mais 3468
AWSQuickSetupSSMManageResourcesExecutionPolicy 3468
Utilização desta política 3468
Detalhes desta política 3468
Versão da política 3468
Documento da política JSON 3469
Saiba mais 3471
AWSQuickSetupStartSSMAssociationsExecutionPolicy 3472
Utilização desta política 3472
Detalhes desta política 3472
Versão da política 3472
Documento da política JSON 3472
Saiba mais 3473

AWSQuickSetupStartStopInstancesExecutionPolicy 3474
Utilização desta política 3474
Detalhes desta política 3474
Versão da política 3474
Documento da política JSON 3474
Saiba mais 3476
AWSQuickSightAssetBundleExportPolicy 3476
Utilização desta política 3476
Detalhes desta política 3476
Versão da política 3477
Documento da política JSON 3477
Saiba mais 3479
AWSQuickSightAssetBundleImportPolicy 3479
Utilização desta política 3479
Detalhes desta política 3479
Versão da política 3480
Documento da política JSON 3480
Saiba mais 3483
AWSQuicksightAthenaAccess 3483
Utilização desta política 3483
Detalhes desta política 3483
Versão da política 3483
Documento da política JSON 3484
Saiba mais 3486
AWSQuickSightDescribeRDS 3486
Utilização desta política 3486
Detalhes desta política 3486
Versão da política 3486
Documento da política JSON 3487
Saiba mais 3487
AWSQuickSightDescribeRedshift 3487
Utilização desta política 3487
Detalhes desta política 3487
Versão da política 3488
Documento da política JSON 3488
Saiba mais 3488

AWSQuickSightElasticsearchPolicy 3488
Utilização desta política 3489
Detalhes desta política 3489
Versão da política 3489
Documento da política JSON 3489
Saiba mais 3490
AWSQuickSightIoTAnalyticsAccess 3490
Utilização desta política 3491
Detalhes desta política 3491
Versão da política 3491
Documento da política JSON 3491
Saiba mais 3491
AWSQuickSightListIAM 3492
Utilização desta política 3492
Detalhes desta política 3492
Versão da política 3492
Documento da política JSON 3492
Saiba mais 3493
AWSQuicksightOpenSearchPolicy 3493
Utilização desta política 3493
Detalhes desta política 3493
Versão da política 3493
Documento da política JSON 3494
Saiba mais 3495
AWSQuickSightSageMakerPolicy 3495
Utilização desta política 3495
Detalhes desta política 3495
Versão da política 3495
Documento da política JSON 3495
Saiba mais 3497
AWSQuickSightSecretsManagerWriteAccess 3497
Utilização desta política 3497
Detalhes desta política 3497
Versão da política 3497
Documento da política JSON 3498
Saiba mais 3498

AWSQuickSightSecretsManagerWritePolicy 3499
Utilização desta política 3499
Detalhes desta política 3499
Versão da política 3499
Documento da política JSON 3499
Saiba mais 3500
AWSQuickSightTimestreamPolicy 3500
Utilização desta política 3501
Detalhes desta política 3501
Versão da política 3501
Documento da política JSON 3501
Saiba mais 3502
AWSReachabilityAnalyzerServiceRolePolicy 3502
Utilização desta política 3502
Detalhes desta política 3502
Versão da política 3502
Documento da política JSON 3503
Saiba mais 3505
AWSRefactoringToolkitFullAccess 3505
Utilização desta política 3505
Detalhes desta política 3505
Versão da política 3506
Documento da política JSON 3506
Saiba mais 3519
AWSRefactoringToolkitSidecarPolicy 3519
Utilização desta política 3520
Detalhes desta política 3520
Versão da política 3520
Documento da política JSON 3520
Saiba mais 3521
AWSrePostPrivateCloudWatchAccess 3521
Utilização desta política 3522
Detalhes desta política 3522
Versão da política 3522
Documento da política JSON 3522
Saiba mais 3523

AWSRepostSpaceSupportOperationsPolicy 3523
Utilização desta política 3523
Detalhes desta política 3523
Versão da política 3523
Documento da política JSON 3524
Saiba mais 3524
AWSResilienceHubAsssessmentExecutionPolicy 3524
Utilização desta política 3524
Detalhes desta política 3525
Versão da política 3525
Documento da política JSON 3525
Saiba mais 3530
AWSResilienceHubResilienceTestingPolicy 3530
Utilização desta política 3530
Detalhes desta política 3530
Versão da política 3530
Documento da política JSON 3531
Saiba mais 3534
AWSResilienceHubServiceRolePolicy 3534
Utilização desta política 3534
Detalhes desta política 3534
Versão da política 3534
Documento da política JSON 3535
Saiba mais 3535
AWSResilienceHubV2AssessmentExecutionPolicy 3535
Utilização desta política 3536
Detalhes desta política 3536
Versão da política 3536
Documento da política JSON 3536
Saiba mais 3542
AWSResourceAccessManagerFullAccess 3542
Utilização desta política 3542
Detalhes desta política 3542
Versão da política 3543
Documento da política JSON 3543
Saiba mais 3543

AWSResourceAccessManagerReadOnlyAccess 3543
Utilização desta política 3544
Detalhes desta política 3544
Versão da política 3544
Documento da política JSON 3544
Saiba mais 3544
AWSResourceAccessManagerResourceShareParticipantAccess 3545
Utilização desta política 3545
Detalhes desta política 3545
Versão da política 3545
Documento da política JSON 3545
Saiba mais 3546
AWSResourceAccessManagerServiceRolePolicy 3546
Utilização desta política 3546
Detalhes desta política 3546
Versão da política 3547
Documento da política JSON 3547
Saiba mais 3548
AWSResourceExplorerFullAccess 3548
Utilização desta política 3548
Detalhes desta política 3548
Versão da política 3548
Documento da política JSON 3549
Saiba mais 3549
AWSResourceExplorerOrganizationsAccess 3550
Utilização desta política 3550
Detalhes desta política 3550
Versão da política 3550
Documento da política JSON 3550
Saiba mais 3552
AWSResourceExplorerReadOnlyAccess 3552
Utilização desta política 3552
Detalhes desta política 3552
Versão da política 3553
Documento da política JSON 3553
Saiba mais 3553

AWSResourceExplorerServiceRolePolicy 3554
Utilização desta política 3554
Detalhes desta política 3554
Versão da política 3554
Documento da política JSON 3554
Saiba mais 3620
AWSResourceGroupsReadOnlyAccess 3620
Utilização desta política 3621
Detalhes desta política 3621
Versão da política 3621
Documento da política JSON 3621
Saiba mais 3622
AWSRevenueAttributionManagement 3623
Utilização desta política 3623
Detalhes desta política 3623
Versão da política 3623
Documento da política JSON 3623
Saiba mais 3625
AWSRoboMaker_FullAccess 3625
Utilização desta política 3625
Detalhes desta política 3626
Versão da política 3626
Documento da política JSON 3626
Saiba mais 3627
AWSRoboMakerReadOnlyAccess 3627
Utilização desta política 3628
Detalhes desta política 3628
Versão da política 3628
Documento da política JSON 3628
Saiba mais 3629
AWSRoboMakerServicePolicy 3629
Utilização desta política 3629
Detalhes desta política 3629
Versão da política 3629
Documento da política JSON 3629
Saiba mais 3631

AWSRoboMakerServiceRolePolicy 3631
Utilização desta política 3631
Detalhes desta política 3631
Versão da política 3632
Documento da política JSON 3632
Saiba mais 3633
AWSRolesAnywhereFullAccess 3633
Utilização desta política 3633
Detalhes desta política 3633
Versão da política 3634
Documento da política JSON 3634
Saiba mais 3636
AWSRolesAnywhereReadOnly 3637
Utilização desta política 3637
Detalhes desta política 3637
Versão da política 3637
Documento da política JSON 3637
Saiba mais 3639
AWSRolesAnywhereServicePolicy 3639
Utilização desta política 3639
Detalhes desta política 3639
Versão da política 3639
Documento da política JSON 3640
Saiba mais 3640
AWSS3OnOutpostsServiceRolePolicy 3641
Utilização desta política 3641
Detalhes desta política 3641
Versão da política 3641
Documento da política JSON 3641
Saiba mais 3644
AWSSavingsPlansFullAccess 3644
Utilização desta política 3644
Detalhes desta política 3644
Versão da política 3644
Documento da política JSON 3645
Saiba mais 3645

AWSSavingsPlansReadOnlyAccess 3645
Utilização desta política 3645
Detalhes desta política 3645
Versão da política 3646
Documento da política JSON 3646
Saiba mais 3646
AWSSDMPServiceRolePolicy 3646
Utilização desta política 3647
Detalhes desta política 3647
Versão da política 3647
Documento da política JSON 3647
Saiba mais 3650
AWSSecretsManagerClientReadOnlyAccess 3650
Utilização desta política 3651
Detalhes desta política 3651
Versão da política 3651
Documento da política JSON 3651
Saiba mais 3652
AWSSecurityAgentServiceRolePolicy 3652
Utilização desta política 3652
Detalhes desta política 3653
Versão da política 3653
Documento da política JSON 3653
Saiba mais 3655
AWSSecurityAgentWebAppPolicy 3655
Utilização desta política 3655
Detalhes desta política 3655
Versão da política 3656
Documento da política JSON 3656
Saiba mais 3658
AWSSecurityHubFullAccess 3658
Utilização desta política 3658
Detalhes desta política 3658
Versão da política 3659
Documento da política JSON 3659
Saiba mais 3660

AWSSecurityHubOrganizationsAccess 3661
Utilização desta política 3661
Detalhes desta política 3661
Versão da política 3661
Documento da política JSON 3661
Saiba mais 3664
AWSSecurityHubReadOnlyAccess 3664
Utilização desta política 3664
Detalhes desta política 3664
Versão da política 3664
Documento da política JSON 3665
Saiba mais 3665
AWSSecurityHubServiceRolePolicy 3665
Utilização desta política 3665
Detalhes desta política 3666
Versão da política 3666
Documento da política JSON 3666
Saiba mais 3669
AWSSecurityHubV2ServiceRolePolicy 3669
Utilização desta política 3669
Detalhes desta política 3669
Versão da política 3670
Documento da política JSON 3670
Saiba mais 3676
AWSSecurityIncidentResponseCaseFullAccess 3676
Utilização desta política 3676
Detalhes desta política 3676
Versão da política 3676
Documento da política JSON 3677
Saiba mais 3678
AWSSecurityIncidentResponseFullAccess 3678
Utilização desta política 3678
Detalhes desta política 3678
Versão da política 3678
Documento da política JSON 3678
Saiba mais 3680

AWSSecurityIncidentResponseReadOnlyAccess 3680
Utilização desta política 3680
Detalhes desta política 3681
Versão da política 3681
Documento da política JSON 3681
Saiba mais 3682
AWSSecurityIncidentResponseServiceRolePolicy 3682
Utilização desta política 3682
Detalhes desta política 3682
Versão da política 3682
Documento da política JSON 3683
Saiba mais 3684
AWSSecurityIncidentResponseTriageServiceRolePolicy 3684
Utilização desta política 3684
Detalhes desta política 3684
Versão da política 3685
Documento da política JSON 3685
Saiba mais 3687
AWSServiceCatalogAdminFullAccess 3687
Utilização desta política 3687
Detalhes desta política 3688
Versão da política 3688
Documento da política JSON 3688
Saiba mais 3691
AWSServiceCatalogAdminReadOnlyAccess 3691
Utilização desta política 3691
Detalhes desta política 3691
Versão da política 3691
Documento da política JSON 3692
Saiba mais 3693
AWSServiceCatalogAppRegistryFullAccess 3693
Utilização desta política 3693
Detalhes desta política 3693
Versão da política 3694
Documento da política JSON 3694
Saiba mais 3696

AWSServiceCatalogAppRegistryReadOnlyAccess 3697
Utilização desta política 3697
Detalhes desta política 3697
Versão da política 3697
Documento da política JSON 3697
Saiba mais 3698
AWSServiceCatalogAppRegistryServiceRolePolicy 3698
Utilização desta política 3698
Detalhes desta política 3698
Versão da política 3699
Documento da política JSON 3699
Saiba mais 3700
AWSServiceCatalogEndUserFullAccess 3700
Utilização desta política 3700
Detalhes desta política 3700
Versão da política 3701
Documento da política JSON 3701
Saiba mais 3703
AWSServiceCatalogEndUserReadOnlyAccess 3703
Utilização desta política 3703
Detalhes desta política 3703
Versão da política 3704
Documento da política JSON 3704
Saiba mais 3705
AWSServiceCatalogOrgsDataSyncServiceRolePolicy 3706
Utilização desta política 3706
Detalhes desta política 3706
Versão da política 3706
Documento da política JSON 3706
Saiba mais 3707
AWSServiceCatalogSyncServiceRolePolicy 3707
Utilização desta política 3707
Detalhes desta política 3708
Versão da política 3708
Documento da política JSON 3708
Saiba mais 3709

AWSServiceRoleForAIDevOpsPolicy 3709
Utilização desta política 3709
Detalhes desta política 3709
Versão da política 3710
Documento da política JSON 3710
Saiba mais 3712
AWSServiceRoleForAmazonEKSNodegroup 3712
Utilização desta política 3713
Detalhes desta política 3713
Versão da política 3713
Documento da política JSON 3713
Saiba mais 3719
AWSServiceRoleForAmazonQDeveloper 3719
Utilização desta política 3719
Detalhes desta política 3719
Versão da política 3719
Documento da política JSON 3720
Saiba mais 3720
AWSServiceRoleForAWSTransform 3720
Utilização desta política 3721
Detalhes desta política 3721
Versão da política 3721
Documento da política JSON 3721
Saiba mais 3723
AWSServiceRoleForAWSTransformCustom 3724
Utilização desta política 3724
Detalhes desta política 3724
Versão da política 3724
Documento da política JSON 3724
Saiba mais 3725
AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy 3725
Utilização desta política 3726
Detalhes desta política 3726
Versão da política 3726
Documento da política JSON 3726
Saiba mais 3727

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy 3727
Utilização desta política 3727
Detalhes desta política 3727
Versão da política 3727
Documento da política JSON 3727
Saiba mais 3728
AWSServiceRoleForCodeGuru-Profiler 3728
Utilização desta política 3728
Detalhes desta política 3728
Versão da política 3729
Documento da política JSON 3729
Saiba mais 3729
AWSServiceRoleForCodeWhispererPolicy 3729
Utilização desta política 3730
Detalhes desta política 3730
Versão da política 3730
Documento da política JSON 3730
Saiba mais 3733
AWSServiceRoleForEC2ScheduledInstances 3733
Utilização desta política 3733
Detalhes desta política 3733
Versão da política 3733
Documento da política JSON 3733
Saiba mais 3734
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy 3735
Utilização desta política 3735
Detalhes desta política 3735
Versão da política 3735
Documento da política JSON 3735
Saiba mais 3736
AWSServiceRoleForImageBuilder 3736
Utilização desta política 3736
Detalhes desta política 3736
Versão da política 3736
Documento da política JSON 3737
Saiba mais 3748

AWSServiceRoleForIoTSiteWise 3748
Utilização desta política 3748
Detalhes desta política 3748
Versão da política 3748
Documento da política JSON 3749
Saiba mais 3750
AWSServiceRoleForLogDeliveryPolicy 3750
Utilização desta política 3750
Detalhes desta política 3750
Versão da política 3751
Documento da política JSON 3751
Saiba mais 3752
AWSServiceRoleForMonitronPolicy 3752
Utilização desta política 3752
Detalhes desta política 3752
Versão da política 3752
Documento da política JSON 3753
Saiba mais 3754
AWSServiceRoleForNeptuneGraphPolicy 3754
Utilização desta política 3754
Detalhes desta política 3754
Versão da política 3755
Documento da política JSON 3755
Saiba mais 3756
AWSServiceRoleForPrivateMarketplaceAdminPolicy 3756
Utilização desta política 3757
Detalhes desta política 3757
Versão da política 3757
Documento da política JSON 3757
Saiba mais 3759
AWSServiceRoleForProcurementInsightsPolicy 3759
Utilização desta política 3759
Detalhes desta política 3759
Versão da política 3759
Documento da política JSON 3760
Saiba mais 3760

AWSServiceRoleForSMS 3760
Utilização desta política 3761
Detalhes desta política 3761
Versão da política 3761
Documento da política JSON 3761
Saiba mais 3768
AWSServiceRoleForUserSubscriptions 3768
Utilização desta política 3768
Detalhes desta política 3768
Versão da política 3768
Documento da política JSON 3769
Saiba mais 3770
AWSServiceRolePolicyForBackupReports 3770
Utilização desta política 3770
Detalhes desta política 3770
Versão da política 3771
Documento da política JSON 3771
Saiba mais 3772
AWSServiceRolePolicyForBackupRestoreTesting 3772
Utilização desta política 3772
Detalhes desta política 3773
Versão da política 3773
Documento da política JSON 3773
Saiba mais 3776
AWSServiceRolePolicyForWorkspacesInstances 3776
Utilização desta política 3776
Detalhes desta política 3776
Versão da política 3777
Documento da política JSON 3777
Saiba mais 3778
AWSShieldDRTAccessPolicy 3779
Utilização desta política 3779
Detalhes desta política 3779
Versão da política 3779
Documento da política JSON 3779
Saiba mais 3780

AWSShieldServiceRolePolicy 3780
Utilização desta política 3781
Detalhes desta política 3781
Versão da política 3781
Documento da política JSON 3781
Saiba mais 3782
AWSSocialMessagingServiceRolePolicy 3782
Utilização desta política 3782
Detalhes desta política 3782
Versão da política 3782
Documento da política JSON 3783
Saiba mais 3783
AWSSSMForSAPServiceLinkedRolePolicy 3783
Utilização desta política 3783
Detalhes desta política 3783
Versão da política 3784
Documento da política JSON 3784
Saiba mais 3792
AWSSSMOpsInsightsServiceRolePolicy 3793
Utilização desta política 3793
Detalhes desta política 3793
Versão da política 3793
Documento da política JSON 3793
Saiba mais 3794
AWSSSODirectoryAdministrator 3794
Utilização desta política 3794
Detalhes desta política 3794
Versão da política 3795
Documento da política JSON 3795
Saiba mais 3796
AWSSSODirectoryReadOnly 3796
Utilização desta política 3796
Detalhes desta política 3796
Versão da política 3796
Documento da política JSON 3797
Saiba mais 3797

AWSSSOMasterAccountAdministrator 3798
Utilização desta política 3798
Detalhes desta política 3798
Versão da política 3798
Documento da política JSON 3798
Saiba mais 3801
AWSSSOMemberAccountAdministrator 3801
Utilização desta política 3802
Detalhes desta política 3802
Versão da política 3802
Documento da política JSON 3802
Saiba mais 3804
AWSSSOReadOnly 3804
Utilização desta política 3805
Detalhes desta política 3805
Versão da política 3805
Documento da política JSON 3805
Saiba mais 3806
AWSSSOServiceRolePolicy 3807
Utilização desta política 3807
Detalhes desta política 3807
Versão da política 3807
Documento da política JSON 3807
Saiba mais 3811
AWSStepFunctionsConsoleFullAccess 3811
Utilização desta política 3811
Detalhes desta política 3812
Versão da política 3812
Documento da política JSON 3812
Saiba mais 3813
AWSStepFunctionsFullAccess 3813
Utilização desta política 3813
Detalhes desta política 3813
Versão da política 3813
Documento da política JSON 3814
Saiba mais 3814

AWSStepFunctionsReadOnlyAccess 3814
Utilização desta política 3814
Detalhes desta política 3814
Versão da política 3815
Documento da política JSON 3815
Saiba mais 3815
AWSStorageGatewayFullAccess 3816
Utilização desta política 3816
Detalhes desta política 3816
Versão da política 3816
Documento da política JSON 3816
Saiba mais 3817
AWSStorageGatewayReadOnlyAccess 3817
Utilização desta política 3817
Detalhes desta política 3817
Versão da política 3818
Documento da política JSON 3818
Saiba mais 3819
AWSStorageGatewayServiceRolePolicy 3819
Utilização desta política 3819
Detalhes desta política 3819
Versão da política 3819
Documento da política JSON 3820
Saiba mais 3820
AWSSupplyChainFederationAdminAccess 3820
Utilização desta política 3820
Detalhes desta política 3820
Versão da política 3821
Documento da política JSON 3821
Saiba mais 3828
AWSSupportAccess 3828
Utilização desta política 3828
Detalhes desta política 3828
Versão da política 3828
Documento da política JSON 3828
Saiba mais 3829

AWSSupportAppFullAccess 3829
Utilização desta política 3829
Detalhes desta política 3829
Versão da política 3830
Documento da política JSON 3830
Saiba mais 3831
AWSSupportAppReadOnlyAccess 3831
Utilização desta política 3831
Detalhes desta política 3831
Versão da política 3831
Documento da política JSON 3831
Saiba mais 3832
AWSSupportPlansFullAccess 3832
Utilização desta política 3832
Detalhes desta política 3832
Versão da política 3832
Documento da política JSON 3833
Saiba mais 3834
AWSSupportPlansReadOnlyAccess 3834
Utilização desta política 3834
Detalhes desta política 3834
Versão da política 3834
Documento da política JSON 3835
Saiba mais 3835
AWSSupportPlansServiceRolePolicy 3835
Utilização desta política 3835
Detalhes desta política 3836
Versão da política 3836
Documento da política JSON 3836
Saiba mais 3837
AWSSupportServiceRolePolicy 3837
Utilização desta política 3837
Detalhes desta política 3837
Versão da política 3837
Documento da política JSON 3837
Saiba mais 3943

AWSSystemsManagerAccountDiscoveryServicePolicy 3943
Utilização desta política 3943
Detalhes desta política 3943
Versão da política 3944
Documento da política JSON 3944
Saiba mais 3944
AWSSystemsManagerChangeManagementServicePolicy 3945
Utilização desta política 3945
Detalhes desta política 3945
Versão da política 3945
Documento da política JSON 3945
Saiba mais 3948
AWSSystemsManagerEnableConfigRecordingExecutionPolicy 3948
Utilização desta política 3948
Detalhes desta política 3948
Versão da política 3948
Documento da política JSON 3949
Saiba mais 3951
AWSSystemsManagerEnableExplorerExecutionPolicy 3951
Utilização desta política 3951
Detalhes desta política 3951
Versão da política 3951
Documento da política JSON 3952
Saiba mais 3953
AWSSystemsManagerForSAPFullAccess 3953
Utilização desta política 3953
Detalhes desta política 3953
Versão da política 3953
Documento da política JSON 3954
Saiba mais 3955
AWSSystemsManagerForSAPReadOnlyAccess 3955
Utilização desta política 3955
Detalhes desta política 3955
Versão da política 3955
Documento da política JSON 3956
Saiba mais 3956

AWSSystemsManagerJustInTimeAccessServicePolicy 3956
Utilização desta política 3956
Detalhes desta política 3957
Versão da política 3957
Documento da política JSON 3957
Saiba mais 3962
AWSSystemsManagerJustInTimeAccessTokenPolicy 3962
Utilização desta política 3963
Detalhes desta política 3963
Versão da política 3963
Documento da política JSON 3963
Saiba mais 3966
AWSSystemsManagerJustInTimeAccessTokenSessionPolicy 3966
Utilização desta política 3966
Detalhes desta política 3966
Versão da política 3967
Documento da política JSON 3967
Saiba mais 3969
AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy 3970
Utilização desta política 3970
Detalhes desta política 3970
Versão da política 3970
Documento da política JSON 3970
Saiba mais 3974
AWSSystemsManagerNotificationsServicePolicy 3975
Utilização desta política 3975
Detalhes desta política 3975
Versão da política 3975
Documento da política JSON 3975
Saiba mais 3977
AWSSystemsManagerOpsDataSyncServiceRolePolicy 3977
Utilização desta política 3977
Detalhes desta política 3977
Versão da política 3977
Documento da política JSON 3978
Saiba mais 3981

AWSThinkboxAssetServerPolicy 3981
Utilização desta política 3981
Detalhes desta política 3982
Versão da política 3982
Documento da política JSON 3982
Saiba mais 3983
AWSThinkboxAWSPortalAdminPolicy 3983
Utilização desta política 3983
Detalhes desta política 3983
Versão da política 3983
Documento da política JSON 3984
Saiba mais 3993
AWSThinkboxAWSPortalGatewayPolicy 3994
Utilização desta política 3994
Detalhes desta política 3994
Versão da política 3994
Documento da política JSON 3994
Saiba mais 3996
AWSThinkboxAWSPortalWorkerPolicy 3996
Utilização desta política 3997
Detalhes desta política 3997
Versão da política 3997
Documento da política JSON 3997
Saiba mais 3999
AWSThinkboxDeadlineResourceTrackerAccessPolicy 3999
Utilização desta política 3999
Detalhes desta política 3999
Versão da política 4000
Documento da política JSON 4000
Saiba mais 4003
AWSThinkboxDeadlineResourceTrackerAdminPolicy 4003
Utilização desta política 4003
Detalhes desta política 4003
Versão da política 4003
Documento da política JSON 4004
Saiba mais 4009

AWSThinkboxDeadlineSpotEventPluginAdminPolicy 4010
Utilização desta política 4010
Detalhes desta política 4010
Versão da política 4010
Documento da política JSON 4010
Saiba mais 4013
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy 4013
Utilização desta política 4013
Detalhes desta política 4014
Versão da política 4014
Documento da política JSON 4014
Saiba mais 4015
AWSTransferConsoleFullAccess 4016
Utilização desta política 4016
Detalhes desta política 4016
Versão da política 4016
Documento da política JSON 4016
Saiba mais 4017
AWSTransferFullAccess 4017
Utilização desta política 4017
Detalhes desta política 4018
Versão da política 4018
Documento da política JSON 4018
Saiba mais 4019
AWSTransferLoggingAccess 4019
Utilização desta política 4019
Detalhes desta política 4019
Versão da política 4019
Documento da política JSON 4020
Saiba mais 4020
AWSTransferReadOnlyAccess 4020
Utilização desta política 4020
Detalhes desta política 4021
Versão da política 4021
Documento da política JSON 4021
Saiba mais 4021

AWSTransferServiceRolePolicy 4022
Utilização desta política 4022
Detalhes desta política 4022
Versão da política 4022
Documento da política JSON 4022
Saiba mais 4024
AWSTransformApplicationDeploymentPolicy 4024
Utilização desta política 4024
Detalhes desta política 4024
Versão da política 4024
Documento da política JSON 4025
Saiba mais 4033
AWSTransformApplicationECSDeploymentPolicy 4033
Utilização desta política 4033
Detalhes desta política 4033
Versão da política 4034
Documento da política JSON 4034
Saiba mais 4042
AWSTransformCustomExecuteTransformations 4042
Utilização desta política 4042
Detalhes desta política 4043
Versão da política 4043
Documento da política JSON 4043
Saiba mais 4044
AWSTransformCustomFullAccess 4044
Utilização desta política 4044
Detalhes desta política 4044
Versão da política 4045
Documento da política JSON 4045
Saiba mais 4046
AWSTransformCustomManageTransformations 4046
Utilização desta política 4046
Detalhes desta política 4046
Versão da política 4046
Documento da política JSON 4046
Saiba mais 4048

AWSTransformInfrastructureExecutorAccessBatch 4048
Utilização desta política 4048
Detalhes desta política 4048
Versão da política 4048
Documento da política JSON 4049
Saiba mais 4055
AWSTransformInfrastructureExecutorAccessEC2 4056
Utilização desta política 4056
Detalhes desta política 4056
Versão da política 4056
Documento da política JSON 4056
Saiba mais 4064
AWSTransformLandingZoneAgentPolicy 4064
Utilização desta política 4064
Detalhes desta política 4064
Versão da política 4064
Documento da política JSON 4065
Saiba mais 4072
AWSTransformNetworkMigrationAgentPolicy 4073
Utilização desta política 4073
Detalhes desta política 4073
Versão da política 4073
Documento da política JSON 4073
Saiba mais 4101
AWSTransformRevenueAttributionPolicy 4101
Utilização desta política 4102
Detalhes desta política 4102
Versão da política 4102
Documento da política JSON 4102
Saiba mais 4103
AWSTransformSecretsManagerConnectorPolicy 4103
Utilização desta política 4103
Detalhes desta política 4103
Versão da política 4103
Documento da política JSON 4104
Saiba mais 4105

AWSTransformSecurityAgentExecutorAccess 4105
Utilização desta política 4105
Detalhes desta política 4105
Versão da política 4106
Documento da política JSON 4106
Saiba mais 4108
AWSTransformServerMigrationAgentPolicy 4108
Utilização desta política 4108
Detalhes desta política 4108
Versão da política 4109
Documento da política JSON 4109
Saiba mais 4133
AWSTrustedAdvisorPriorityFullAccess 4133
Utilização desta política 4133
Detalhes desta política 4133
Versão da política 4133
Documento da política JSON 4134
Saiba mais 4135
AWSTrustedAdvisorPriorityReadOnlyAccess 4136
Utilização desta política 4136
Detalhes desta política 4136
Versão da política 4136
Documento da política JSON 4136
Saiba mais 4137
AWSTrustedAdvisorReportingServiceRolePolicy 4137
Utilização desta política 4138
Detalhes desta política 4138
Versão da política 4138
Documento da política JSON 4138
Saiba mais 4139
AWSTrustedAdvisorServiceRolePolicy 4139
Utilização desta política 4139
Detalhes desta política 4139
Versão da política 4139
Documento da política JSON 4140
Saiba mais 4143

AWSUserAttributeCostAllocationPolicy 4143
Utilização desta política 4143
Detalhes desta política 4143
Versão da política 4143
Documento da política JSON 4144
Saiba mais 4144
AWSUserNotificationsServiceLinkedRolePolicy 4144
Utilização desta política 4144
Detalhes desta política 4144
Versão da política 4145
Documento da política JSON 4145
Saiba mais 4146
AWSVendorInsightsAssessorFullAccess 4147
Utilização desta política 4147
Detalhes desta política 4147
Versão da política 4147
Documento da política JSON 4147
Saiba mais 4148
AWSVendorInsightsAssessorReadOnly 4149
Utilização desta política 4149
Detalhes desta política 4149
Versão da política 4149
Documento da política JSON 4149
Saiba mais 4150
AWSVendorInsightsVendorFullAccess 4150
Utilização desta política 4150
Detalhes desta política 4150
Versão da política 4151
Documento da política JSON 4151
Saiba mais 4152
AWSVendorInsightsVendorReadOnly 4153
Utilização desta política 4153
Detalhes desta política 4153
Versão da política 4153
Documento da política JSON 4153
Saiba mais 4154

AWSVPCFlowLogsServiceRolePolicy 4154
Utilização desta política 4155
Detalhes desta política 4155
Versão da política 4155
Documento da política JSON 4155
Saiba mais 4157
AWSVpcLatticeServiceRolePolicy 4157
Utilização desta política 4157
Detalhes desta política 4157
Versão da política 4157
Documento da política JSON 4157
Saiba mais 4160
AWSVPCS2SVpnServiceRolePolicy 4160
Utilização desta política 4160
Detalhes desta política 4161
Versão da política 4161
Documento da política JSON 4161
Saiba mais 4162
AWSVPCTransitGatewayServiceRolePolicy 4162
Utilização desta política 4162
Detalhes desta política 4163
Versão da política 4163
Documento da política JSON 4163
Saiba mais 4164
AWSVPCVerifiedAccessServiceRolePolicy 4164
Utilização desta política 4164
Detalhes desta política 4164
Versão da política 4164
Documento da política JSON 4164
Saiba mais 4166
AWSWAFConsoleFullAccess 4166
Utilização desta política 4166
Detalhes desta política 4167
Versão da política 4167
Documento da política JSON 4167
Saiba mais 4176

AWSWAFConsoleReadOnlyAccess 4176
Utilização desta política 4177
Detalhes desta política 4177
Versão da política 4177
Documento da política JSON 4177
Saiba mais 4185
AWSWAFFullAccess 4185
Utilização desta política 4185
Detalhes desta política 4185
Versão da política 4185
Documento da política JSON 4185
Saiba mais 4191
AWSWAFReadOnlyAccess 4192
Utilização desta política 4192
Detalhes desta política 4192
Versão da política 4192
Documento da política JSON 4192
Saiba mais 4196
AWSWellArchitectedAgentOrganizationsServiceRolePolicy 4197
Utilização desta política 4197
Detalhes desta política 4197
Versão da política 4197
Documento da política JSON 4197
Saiba mais 4198
AWSWellArchitectedAgentResourceScanningServiceRolePolicy 4198
Utilização desta política 4198
Detalhes desta política 4199
Versão da política 4199
Documento da política JSON 4199
Saiba mais 4263
AWSWellArchitectedDiscoveryServiceRolePolicy 4263
Utilização desta política 4264
Detalhes desta política 4264
Versão da política 4264
Documento da política JSON 4264
Saiba mais 4266

AWSWellArchitectedOrganizationsServiceRolePolicy 4266
Utilização desta política 4266
Detalhes desta política 4266
Versão da política 4266
Documento da política JSON 4266
Saiba mais 4267
AWSWickrFullAccess 4267
Utilização desta política 4267
Detalhes desta política 4267
Versão da política 4268
Documento da política JSON 4268
Saiba mais 4268
AWSXrayCrossAccountSharingConfiguration 4268
Utilização desta política 4269
Detalhes desta política 4269
Versão da política 4269
Documento da política JSON 4269
Saiba mais 4270
AWSXRayDaemonWriteAccess 4270
Utilização desta política 4270
Detalhes desta política 4270
Versão da política 4271
Documento da política JSON 4271
Saiba mais 4271
AWSXrayFullAccess 4272
Utilização desta política 4272
Detalhes desta política 4272
Versão da política 4272
Documento da política JSON 4272
Saiba mais 4273
AWSXrayReadOnlyAccess 4273
Utilização desta política 4273
Detalhes desta política 4273
Versão da política 4273
Documento da política JSON 4274
Saiba mais 4274

AWSXrayWriteOnlyAccess 4275
Utilização desta política 4275
Detalhes desta política 4275
Versão da política 4275
Documento da política JSON 4275
Saiba mais 4276
AWSZonalAutoshiftPracticeRunSLRPolicy 4276
Utilização desta política 4276
Detalhes desta política 4276
Versão da política 4276
Documento da política JSON 4277
Saiba mais 4278
AWSZoneGroupAccessManagementServiceRolePolicy 4278
Utilização desta política 4278
Detalhes desta política 4278
Versão da política 4278
Documento da política JSON 4278
Saiba mais 4279
BatchServiceRolePolicy 4279
Utilização desta política 4279
Detalhes desta política 4279
Versão da política 4280
Documento da política JSON 4280
Saiba mais 4287
BedrockAgentCoreFullAccess 4287
Utilização desta política 4287
Detalhes desta política 4287
Versão da política 4287
Documento da política JSON 4287
Saiba mais 4299
BedrockAgentCoreNetworkServiceRolePolicy 4299
Utilização desta política 4299
Detalhes desta política 4299
Versão da política 4299
Documento da política JSON 4300
Saiba mais 4302

BedrockAgentCoreRuntimeIdentityServiceRolePolicy 4302
Utilização desta política 4302
Detalhes desta política 4302
Versão da política 4302
Documento da política JSON 4303
Saiba mais 4303
BedrockAgentCoreRuntimeInstancesInstanceRolePolicy 4303
Utilização desta política 4303
Detalhes desta política 4304
Versão da política 4304
Documento da política JSON 4304
Saiba mais 4304
BedrockAgentCoreRuntimeInstancesOperatorRolePolicy 4305
Utilização desta política 4305
Detalhes desta política 4305
Versão da política 4305
Documento da política JSON 4305
Saiba mais 4312
Billing 4313
Utilização desta política 4313
Detalhes desta política 4313
Versão da política 4313
Documento da política JSON 4313
Saiba mais 4317
BudgetsServiceRolePolicy 4317
Utilização desta política 4318
Detalhes desta política 4318
Versão da política 4318
Documento da política JSON 4318
Saiba mais 4318
CertificateManagerServiceRolePolicy 4319
Utilização desta política 4319
Detalhes desta política 4319
Versão da política 4319
Documento da política JSON 4319
Saiba mais 4320

ClientVPNServiceConnectionsRolePolicy 4320
Utilização desta política 4320
Detalhes desta política 4320
Versão da política 4320
Documento da política JSON 4321
Saiba mais 4321
ClientVPNServiceRolePolicy 4321
Utilização desta política 4321
Detalhes desta política 4321
Versão da política 4322
Documento da política JSON 4322
Saiba mais 4323
CloudFormationStackSetsOrgAdminServiceRolePolicy 4323
Utilização desta política 4323
Detalhes desta política 4323
Versão da política 4323
Documento da política JSON 4324
Saiba mais 4324
CloudFormationStackSetsOrgMemberServiceRolePolicy 4324
Utilização desta política 4325
Detalhes desta política 4325
Versão da política 4325
Documento da política JSON 4325
Saiba mais 4327
CloudFrontFullAccess 4327
Utilização desta política 4327
Detalhes desta política 4327
Versão da política 4327
Documento da política JSON 4327
Saiba mais 4329
CloudFrontReadOnlyAccess 4330
Utilização desta política 4330
Detalhes desta política 4330
Versão da política 4330
Documento da política JSON 4330
Saiba mais 4331

CloudHSMServiceRolePolicy 4331
Utilização desta política 4331
Detalhes desta política 4332
Versão da política 4332
Documento da política JSON 4332
Saiba mais 4332
CloudSearchFullAccess 4333
Utilização desta política 4333
Detalhes desta política 4333
Versão da política 4333
Documento da política JSON 4333
Saiba mais 4334
CloudSearchReadOnlyAccess 4334
Utilização desta política 4334
Detalhes desta política 4334
Versão da política 4334
Documento da política JSON 4334
Saiba mais 4335
CloudTrailEventContext 4335
Utilização desta política 4335
Detalhes desta política 4335
Versão da política 4336
Documento da política JSON 4336
Saiba mais 4337
CloudTrailServiceRolePolicy 4338
Utilização desta política 4338
Detalhes desta política 4338
Versão da política 4338
Documento da política JSON 4338
Saiba mais 4340
CloudWatch-CrossAccountAccess 4340
Utilização desta política 4340
Detalhes desta política 4340
Versão da política 4341
Documento da política JSON 4341
Saiba mais 4341

CloudWatchActionsEC2Access 4341
Utilização desta política 4341
Detalhes desta política 4342
Versão da política 4342
Documento da política JSON 4342
Saiba mais 4342
CloudWatchAgentAdminPolicy 4343
Utilização desta política 4343
Detalhes desta política 4343
Versão da política 4343
Documento da política JSON 4343
Saiba mais 4344
CloudWatchAgentServerPolicy 4344
Utilização desta política 4345
Detalhes desta política 4345
Versão da política 4345
Documento da política JSON 4345
Saiba mais 4346
CloudWatchAPIKeyAccess 4346
Utilização desta política 4346
Detalhes desta política 4346
Versão da política 4347
Documento da política JSON 4347
Saiba mais 4348
CloudWatchApplicationInsightsFullAccess 4348
Utilização desta política 4348
Detalhes desta política 4348
Versão da política 4348
Documento da política JSON 4348
Saiba mais 4350
CloudWatchApplicationInsightsReadOnlyAccess 4350
Utilização desta política 4350
Detalhes desta política 4350
Versão da política 4350
Documento da política JSON 4351
Saiba mais 4351

CloudwatchApplicationInsightsServiceLinkedRolePolicy 4351
Utilização desta política 4351
Detalhes desta política 4352
Versão da política 4352
Documento da política JSON 4352
Saiba mais 4362
CloudWatchApplicationSignalsFullAccess 4363
Utilização desta política 4363
Detalhes desta política 4363
Versão da política 4363
Documento da política JSON 4363
Saiba mais 4368
CloudWatchApplicationSignalsReadOnlyAccess 4369
Utilização desta política 4369
Detalhes desta política 4369
Versão da política 4369
Documento da política JSON 4369
Saiba mais 4373
CloudWatchApplicationSignalsServiceRolePolicy 4374
Utilização desta política 4374
Detalhes desta política 4374
Versão da política 4374
Documento da política JSON 4374
Saiba mais 4377
CloudWatchAutomaticDashboardsAccess 4378
Utilização desta política 4378
Detalhes desta política 4378
Versão da política 4378
Documento da política JSON 4378
Saiba mais 4380
CloudWatchCrossAccountSharingConfiguration 4380
Utilização desta política 4380
Detalhes desta política 4380
Versão da política 4380
Documento da política JSON 4381
Saiba mais 4381

CloudWatchEventsBuiltInTargetExecutionAccess 4382
Utilização desta política 4382
Detalhes desta política 4382
Versão da política 4382
Documento da política JSON 4382
Saiba mais 4383
CloudWatchEventsFullAccess 4383
Utilização desta política 4383
Detalhes desta política 4383
Versão da política 4383
Documento da política JSON 4384
Saiba mais 4386
CloudWatchEventsInvocationAccess 4386
Utilização desta política 4386
Detalhes desta política 4386
Versão da política 4386
Documento da política JSON 4387
Saiba mais 4387
CloudWatchEventsReadOnlyAccess 4387
Utilização desta política 4387
Detalhes desta política 4387
Versão da política 4388
Documento da política JSON 4388
Saiba mais 4389
CloudWatchEventsServiceRolePolicy 4389
Utilização desta política 4390
Detalhes desta política 4390
Versão da política 4390
Documento da política JSON 4390
Saiba mais 4391
CloudWatchFullAccess 4391
Utilização desta política 4391
Detalhes desta política 4391
Versão da política 4391
Documento da política JSON 4392
Saiba mais 4393

CloudWatchFullAccessV2 4393
Utilização desta política 4393
Detalhes desta política 4393
Versão da política 4393
Documento da política JSON 4393
Saiba mais 4399
CloudWatchInternetMonitorFullAccess 4400
Utilização desta política 4400
Detalhes desta política 4400
Versão da política 4400
Documento da política JSON 4400
Saiba mais 4402
CloudWatchInternetMonitorReadOnlyAccess 4402
Utilização desta política 4403
Detalhes desta política 4403
Versão da política 4403
Documento da política JSON 4403
Saiba mais 4404
CloudWatchInternetMonitorServiceRolePolicy 4404
Utilização desta política 4404
Detalhes desta política 4404
Versão da política 4405
Documento da política JSON 4405
Saiba mais 4406
CloudWatchLambdaApplicationSignalsExecutionRolePolicy 4406
Utilização desta política 4406
Detalhes desta política 4406
Versão da política 4407
Documento da política JSON 4407
Saiba mais 4408
CloudWatchLambdaInsightsExecutionRolePolicy 4408
Utilização desta política 4408
Detalhes desta política 4408
Versão da política 4408
Documento da política JSON 4409
Saiba mais 4409

CloudWatchLogsAPIKeyAccess 4409
Utilização desta política 4409
Detalhes desta política 4410
Versão da política 4410
Documento da política JSON 4410
Saiba mais 4411
CloudWatchLogsCrossAccountSharingConfiguration 4411
Utilização desta política 4411
Detalhes desta política 4412
Versão da política 4412
Documento da política JSON 4412
Saiba mais 4413
CloudWatchLogsFullAccess 4413
Utilização desta política 4413
Detalhes desta política 4413
Versão da política 4414
Documento da política JSON 4414
Saiba mais 4414
CloudWatchLogsReadOnlyAccess 4414
Utilização desta política 4415
Detalhes desta política 4415
Versão da política 4415
Documento da política JSON 4415
Saiba mais 4416
CloudWatchNetworkFlowMonitorAgentPublishPolicy 4416
Utilização desta política 4416
Detalhes desta política 4416
Versão da política 4417
Documento da política JSON 4417
Saiba mais 4417
CloudWatchNetworkFlowMonitorServiceRolePolicy 4417
Utilização desta política 4418
Detalhes desta política 4418
Versão da política 4418
Documento da política JSON 4418
Saiba mais 4419

CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy 4419
Utilização desta política 4420
Detalhes desta política 4420
Versão da política 4420
Documento da política JSON 4420
Saiba mais 4423
CloudWatchNetworkMonitorServiceRolePolicy 4423
Utilização desta política 4423
Detalhes desta política 4423
Versão da política 4423
Documento da política JSON 4424
Saiba mais 4425
CloudWatchOmniAWSIntegrationPolicy 4425
Utilização desta política 4425
Detalhes desta política 4425
Versão da política 4426
Documento da política JSON 4426
Saiba mais 4438
CloudWatchOmniDomainAccessPolicy 4438
Utilização desta política 4439
Detalhes desta política 4439
Versão da política 4439
Documento da política JSON 4439
Saiba mais 4440
CloudWatchOmniModelInferencePolicy 4440
Utilização desta política 4440
Detalhes desta política 4440
Versão da política 4440
Documento da política JSON 4441
Saiba mais 4442
CloudWatchOmniSpaceAccessPolicy 4442
Utilização desta política 4442
Detalhes desta política 4442
Versão da política 4442
Documento da política JSON 4443
Saiba mais 4454

CloudWatchOpenSearchDashboardAccess 4454
Utilização desta política 4454
Detalhes desta política 4454
Versão da política 4454
Documento da política JSON 4455
Saiba mais 4457
CloudWatchOpenSearchDashboardsFullAccess 4457
Utilização desta política 4457
Detalhes desta política 4458
Versão da política 4458
Documento da política JSON 4458
Saiba mais 4465
CloudWatchReadOnlyAccess 4465
Utilização desta política 4465
Detalhes desta política 4465
Versão da política 4466
Documento da política JSON 4466
Saiba mais 4469
CloudWatchSyntheticsFullAccess 4469
Utilização desta política 4469
Detalhes desta política 4469
Versão da política 4469
Documento da política JSON 4470
Saiba mais 4475
CloudWatchSyntheticsReadOnlyAccess 4475
Utilização desta política 4475
Detalhes desta política 4475
Versão da política 4476
Documento da política JSON 4476
Saiba mais 4476
ComprehendDataAccessRolePolicy 4476
Utilização desta política 4477
Detalhes desta política 4477
Versão da política 4477
Documento da política JSON 4477
Saiba mais 4478

ComprehendFullAccess 4478
Utilização desta política 4478
Detalhes desta política 4478
Versão da política 4478
Documento da política JSON 4478
Saiba mais 4479
ComprehendMedicalFullAccess 4479
Utilização desta política 4479
Detalhes desta política 4479
Versão da política 4480
Documento da política JSON 4480
Saiba mais 4480
ComprehendReadOnly 4480
Utilização desta política 4480
Detalhes desta política 4481
Versão da política 4481
Documento da política JSON 4481
Saiba mais 4482
ComputeOptimizerAutomationServiceRolePolicy 4482
Utilização desta política 4483
Detalhes desta política 4483
Versão da política 4483
Documento da política JSON 4483
Saiba mais 4485
ComputeOptimizerReadOnlyAccess 4485
Utilização desta política 4485
Detalhes desta política 4485
Versão da política 4485
Documento da política JSON 4486
Saiba mais 4487
ComputeOptimizerServiceRolePolicy 4487
Utilização desta política 4487
Detalhes desta política 4487
Versão da política 4488
Documento da política JSON 4488
Saiba mais 4490

ConfigConformsServiceRolePolicy 4490
Utilização desta política 4491
Detalhes desta política 4491
Versão da política 4491
Documento da política JSON 4491
Saiba mais 4494
ConsoleFullAccessFromVercel 4494
Utilização desta política 4494
Detalhes desta política 4494
Versão da política 4495
Documento da política JSON 4495
Saiba mais 4499
ConsoleViewOnlyAccessFromVercel 4500
Utilização desta política 4500
Detalhes desta política 4500
Versão da política 4500
Documento da política JSON 4500
Saiba mais 4503
CostOptimizationHubAdminAccess 4503
Utilização desta política 4503
Detalhes desta política 4503
Versão da política 4504
Documento da política JSON 4504
Saiba mais 4505
CostOptimizationHubReadOnlyAccess 4505
Utilização desta política 4505
Detalhes desta política 4505
Versão da política 4506
Documento da política JSON 4506
Saiba mais 4506
CostOptimizationHubServiceRolePolicy 4507
Utilização desta política 4507
Detalhes desta política 4507
Versão da política 4507
Documento da política JSON 4507
Saiba mais 4508

CustomerProfilesServiceLinkedRolePolicy 4509
Utilização desta política 4509
Detalhes desta política 4509
Versão da política 4509
Documento da política JSON 4509
Saiba mais 4510
DatabaseAdministrator 4511
Utilização desta política 4511
Detalhes desta política 4511
Versão da política 4511
Documento da política JSON 4511
Saiba mais 4514
DataScientist 4514
Utilização desta política 4514
Detalhes desta política 4514
Versão da política 4515
Documento da política JSON 4515
Saiba mais 4519
DAXServiceRolePolicy 4519
Utilização desta política 4519
Detalhes desta política 4520
Versão da política 4520
Documento da política JSON 4520
Saiba mais 4521
DBModDiscoveryAndAssessment 4521
Utilização desta política 4521
Detalhes desta política 4521
Versão da política 4521
Documento da política JSON 4521
Saiba mais 4525
DBModProvisioningAndMigration 4526
Utilização desta política 4526
Detalhes desta política 4526
Versão da política 4526
Documento da política JSON 4526
Saiba mais 4531

DBModVirtualSource 4531
Utilização desta política 4531
Detalhes desta política 4531
Versão da política 4532
Documento da política JSON 4532
Saiba mais 4536
DeclarativePoliciesEC2Report 4536
Utilização desta política 4536
Detalhes desta política 4537
Versão da política 4537
Documento da política JSON 4537
Saiba mais 4538
DynamoDBCloudWatchContributorInsightsServiceRolePolicy 4538
Utilização desta política 4538
Detalhes desta política 4538
Versão da política 4538
Documento da política JSON 4539
Saiba mais 4539
DynamoDBGlobalTableSettingsManagementServiceRolePolicy 4539
Utilização desta política 4540
Detalhes desta política 4540
Versão da política 4540
Documento da política JSON 4540
Saiba mais 4541
DynamoDBKinesisReplicationServiceRolePolicy 4541
Utilização desta política 4542
Detalhes desta política 4542
Versão da política 4542
Documento da política JSON 4542
Saiba mais 4543
DynamoDBReplicationServiceRolePolicy 4543
Utilização desta política 4543
Detalhes desta política 4543
Versão da política 4543
Documento da política JSON 4544
Saiba mais 4545

EC2ApplicationStatusChecksServiceRolePolicy 4545
Utilização desta política 4545
Detalhes desta política 4545
Versão da política 4546
Documento da política JSON 4546
Saiba mais 4547
EC2FastLaunchFullAccess 4547
Utilização desta política 4547
Detalhes desta política 4547
Versão da política 4547
Documento da política JSON 4548
Saiba mais 4555
EC2FastLaunchServiceRolePolicy 4555
Utilização desta política 4555
Detalhes desta política 4555
Versão da política 4556
Documento da política JSON 4556
Saiba mais 4562
EC2FleetTimeShiftableServiceRolePolicy 4562
Utilização desta política 4562
Detalhes desta política 4562
Versão da política 4562
Documento da política JSON 4563
Saiba mais 4564
Ec2ImageBuilderCrossAccountDistributionAccess 4564
Utilização desta política 4564
Detalhes desta política 4564
Versão da política 4565
Documento da política JSON 4565
Saiba mais 4565
EC2ImageBuilderExecutionPolicy 4566
Utilização desta política 4566
Detalhes desta política 4566
Versão da política 4566
Documento da política JSON 4566
Saiba mais 4582

EC2ImageBuilderLifecycleExecutionPolicy 4582
Utilização desta política 4582
Detalhes desta política 4582
Versão da política 4582
Documento da política JSON 4583
Saiba mais 4584
EC2InstanceConnect 4585
Utilização desta política 4585
Detalhes desta política 4585
Versão da política 4585
Documento da política JSON 4585
Saiba mais 4586
Ec2InstanceConnectEndpoint 4586
Utilização desta política 4586
Detalhes desta política 4586
Versão da política 4586
Documento da política JSON 4587
Saiba mais 4589
EC2InstanceProfileForImageBuilder 4589
Utilização desta política 4590
Detalhes desta política 4590
Versão da política 4590
Documento da política JSON 4590
Saiba mais 4593
EC2InstanceProfileForImageBuilderECRContainerBuilds 4593
Utilização desta política 4593
Detalhes desta política 4593
Versão da política 4593
Documento da política JSON 4594
Saiba mais 4595
ECRReplicationServiceRolePolicy 4595
Utilização desta política 4595
Detalhes desta política 4595
Versão da política 4596
Documento da política JSON 4596
Saiba mais 4596

ECRTemplateServiceRolePolicy 4596
Utilização desta política 4597
Detalhes desta política 4597
Versão da política 4597
Documento da política JSON 4597
Saiba mais 4598
ElastiCacheServiceRolePolicy 4598
Utilização desta política 4598
Detalhes desta política 4598
Versão da política 4598
Documento da política JSON 4598
Saiba mais 4600
ElasticLoadBalancingFullAccess 4601
Utilização desta política 4601
Detalhes desta política 4601
Versão da política 4601
Documento da política JSON 4601
Saiba mais 4603
ElasticLoadBalancingReadOnly 4603
Utilização desta política 4603
Detalhes desta política 4603
Versão da política 4603
Documento da política JSON 4604
Saiba mais 4605
ElementalActivationsDownloadSoftwareAccess 4605
Utilização desta política 4605
Detalhes desta política 4605
Versão da política 4605
Documento da política JSON 4605
Saiba mais 4606
ElementalActivationsFullAccess 4606
Utilização desta política 4606
Detalhes desta política 4606
Versão da política 4607
Documento da política JSON 4607
Saiba mais 4607

ElementalActivationsGenerateLicenses 4607
Utilização desta política 4608
Detalhes desta política 4608
Versão da política 4608
Documento da política JSON 4608
Saiba mais 4609
ElementalActivationsReadOnlyAccess 4609
Utilização desta política 4609
Detalhes desta política 4609
Versão da política 4609
Documento da política JSON 4609
Saiba mais 4610
ElementalAppliancesSoftwareFullAccess 4610
Utilização desta política 4610
Detalhes desta política 4610
Versão da política 4611
Documento da política JSON 4611
Saiba mais 4611
ElementalAppliancesSoftwareReadOnlyAccess 4611
Utilização desta política 4612
Detalhes desta política 4612
Versão da política 4612
Documento da política JSON 4612
Saiba mais 4612
ElementalSupportCenterFullAccess 4613
Utilização desta política 4613
Detalhes desta política 4613
Versão da política 4613
Documento da política JSON 4613
Saiba mais 4614
EMRDescribeClusterPolicyForEMRWAL 4614
Utilização desta política 4614
Detalhes desta política 4614
Versão da política 4615
Documento da política JSON 4615
Saiba mais 4615

EndUserMessagingServiceRolePolicy 4615
Utilização desta política 4615
Detalhes desta política 4616
Versão da política 4616
Documento da política JSON 4616
Saiba mais 4616
FinOpsAgentAgentPolicy 4617
Utilização desta política 4617
Detalhes desta política 4617
Versão da política 4617
Documento da política JSON 4617
Saiba mais 4621
FinOpsAgentOperatorPolicy 4622
Utilização desta política 4622
Detalhes desta política 4622
Versão da política 4622
Documento da política JSON 4622
Saiba mais 4623
FMSServiceRolePolicy 4624
Utilização desta política 4624
Detalhes desta política 4624
Versão da política 4624
Documento da política JSON 4624
Saiba mais 4641
FSxDeleteServiceLinkedRoleAccess 4641
Utilização desta política 4641
Detalhes desta política 4641
Versão da política 4642
Documento da política JSON 4642
Saiba mais 4642
GameLiftContainerFleetPolicy 4642
Utilização desta política 4643
Detalhes desta política 4643
Versão da política 4643
Documento da política JSON 4643
Saiba mais 4644

GameLiftGameServerGroupPolicy 4644
Utilização desta política 4645
Detalhes desta política 4645
Versão da política 4645
Documento da política JSON 4645
Saiba mais 4647
GitLabDuoWithAmazonQPermissionsPolicy 4647
Utilização desta política 4647
Detalhes desta política 4647
Versão da política 4647
Documento da política JSON 4648
Saiba mais 4649
GlobalAcceleratorFullAccess 4649
Utilização desta política 4649
Detalhes desta política 4649
Versão da política 4649
Documento da política JSON 4649
Saiba mais 4650
GlobalAcceleratorReadOnlyAccess 4651
Utilização desta política 4651
Detalhes desta política 4651
Versão da política 4651
Documento da política JSON 4651
Saiba mais 4652
GreengrassOTAUpdateArtifactAccess 4652
Utilização desta política 4652
Detalhes desta política 4652
Versão da política 4652
Documento da política JSON 4653
Saiba mais 4653
GroundTruthSyntheticConsoleFullAccess 4653
Utilização desta política 4653
Detalhes desta política 4654
Versão da política 4654
Documento da política JSON 4654
Saiba mais 4654

GroundTruthSyntheticConsoleReadOnlyAccess 4655
Utilização desta política 4655
Detalhes desta política 4655
Versão da política 4655
Documento da política JSON 4655
Saiba mais 4656
Health_OrganizationsServiceRolePolicy 4656
Utilização desta política 4656
Detalhes desta política 4656
Versão da política 4656
Documento da política JSON 4657
Saiba mais 4657
IAMAccessAdvisorReadOnly 4657
Utilização desta política 4657
Detalhes desta política 4658
Versão da política 4658
Documento da política JSON 4658
Saiba mais 4659
IAMAccessAnalyzerFullAccess 4659
Utilização desta política 4659
Detalhes desta política 4659
Versão da política 4660
Documento da política JSON 4660
Saiba mais 4661
IAMAccessAnalyzerReadOnlyAccess 4661
Utilização desta política 4661
Detalhes desta política 4661
Versão da política 4661
Documento da política JSON 4662
Saiba mais 4662
IAMFullAccess 4662
Utilização desta política 4662
Detalhes desta política 4663
Versão da política 4663
Documento da política JSON 4663
Saiba mais 4664

IAMReadOnlyAccess 4664
Utilização desta política 4664
Detalhes desta política 4664
Versão da política 4664
Documento da política JSON 4664
Saiba mais 4665
IAMSelfManageServiceSpecificCredentials 4665
Utilização desta política 4665
Detalhes desta política 4665
Versão da política 4666
Documento da política JSON 4666
Saiba mais 4666
IAMUserChangePassword 4667
Utilização desta política 4667
Detalhes desta política 4667
Versão da política 4667
Documento da política JSON 4667
Saiba mais 4668
IAMUserSSHKeys 4668
Utilização desta política 4668
Detalhes desta política 4668
Versão da política 4668
Documento da política JSON 4669
Saiba mais 4669
IVSFullAccess 4669
Utilização desta política 4670
Detalhes desta política 4670
Versão da política 4670
Documento da política JSON 4670
Saiba mais 4670
IVSReadOnlyAccess 4671
Utilização desta política 4671
Detalhes desta política 4671
Versão da política 4671
Documento da política JSON 4671
Saiba mais 4673

IVSRecordToS3 4673
Utilização desta política 4673
Detalhes desta política 4673
Versão da política 4673
Documento da política JSON 4674
Saiba mais 4674
KafkaConnectServiceRolePolicy 4674
Utilização desta política 4674
Detalhes desta política 4674
Versão da política 4675
Documento da política JSON 4675
Saiba mais 4676
KafkaServiceRolePolicy 4676
Utilização desta política 4677
Detalhes desta política 4677
Versão da política 4677
Documento da política JSON 4677
Saiba mais 4679
KeyspacesCDCServiceRolePolicy 4679
Utilização desta política 4679
Detalhes desta política 4679
Versão da política 4680
Documento da política JSON 4680
Saiba mais 4680
KeyspacesReplicationServiceRolePolicy 4681
Utilização desta política 4681
Detalhes desta política 4681
Versão da política 4681
Documento da política JSON 4681
Saiba mais 4683
LakeFormationDataAccessServiceRolePolicy 4683
Utilização desta política 4683
Detalhes desta política 4683
Versão da política 4683
Documento da política JSON 4683
Saiba mais 4684

LexBotPolicy 4684
Utilização desta política 4684
Detalhes desta política 4684
Versão da política 4685
Documento da política JSON 4685
Saiba mais 4685
LexChannelPolicy 4686
Utilização desta política 4686
Detalhes desta política 4686
Versão da política 4686
Documento da política JSON 4686
Saiba mais 4687
LightsailExportAccess 4687
Utilização desta política 4687
Detalhes desta política 4687
Versão da política 4687
Documento da política JSON 4687
Saiba mais 4688
MediaConnectGatewayInstanceRolePolicy 4688
Utilização desta política 4689
Detalhes desta política 4689
Versão da política 4689
Documento da política JSON 4689
Saiba mais 4690
MediaPackageServiceRolePolicy 4690
Utilização desta política 4690
Detalhes desta política 4690
Versão da política 4690
Documento da política JSON 4691
Saiba mais 4691
MemoryDBServiceRolePolicy 4691
Utilização desta política 4691
Detalhes desta política 4692
Versão da política 4692
Documento da política JSON 4692
Saiba mais 4694

MigrationHubDMSAccessServiceRolePolicy 4694
Utilização desta política 4695
Detalhes desta política 4695
Versão da política 4695
Documento da política JSON 4695
Saiba mais 4696
MigrationHubServiceRolePolicy 4696
Utilização desta política 4696
Detalhes desta política 4696
Versão da política 4697
Documento da política JSON 4697
Saiba mais 4698
MigrationHubSMSAccessServiceRolePolicy 4698
Utilização desta política 4699
Detalhes desta política 4699
Versão da política 4699
Documento da política JSON 4699
Saiba mais 4700
MonitronServiceRolePolicy 4700
Utilização desta política 4700
Detalhes desta política 4701
Versão da política 4701
Documento da política JSON 4701
Saiba mais 4701
MultiPartyApprovalFullAccess 4702
Utilização desta política 4702
Detalhes desta política 4702
Versão da política 4702
Documento da política JSON 4702
Saiba mais 4705
MultiPartyApprovalReadOnlyAccess 4705
Utilização desta política 4705
Detalhes desta política 4705
Versão da política 4705
Documento da política JSON 4705
Saiba mais 4707

NeptuneConsoleFullAccess 4707
Utilização desta política 4708
Detalhes desta política 4708
Versão da política 4708
Documento da política JSON 4708
Saiba mais 4714
NeptuneFullAccess 4714
Utilização desta política 4714
Detalhes desta política 4714
Versão da política 4714
Documento da política JSON 4714
Saiba mais 4718
NeptuneGraphReadOnlyAccess 4719
Utilização desta política 4719
Detalhes desta política 4719
Versão da política 4719
Documento da política JSON 4719
Saiba mais 4721
NeptuneReadOnlyAccess 4721
Utilização desta política 4721
Detalhes desta política 4721
Versão da política 4721
Documento da política JSON 4722
Saiba mais 4724
NetworkAdministrator 4724
Utilização desta política 4724
Detalhes desta política 4724
Versão da política 4724
Documento da política JSON 4725
Saiba mais 4732
NetworkSecurityDirectorServiceLinkedRolePolicy 4732
Utilização desta política 4732
Detalhes desta política 4732
Versão da política 4733
Documento da política JSON 4733
Saiba mais 4738

NetworkSecurityManagerServiceRolePolicy 4738
Utilização desta política 4739
Detalhes desta política 4739
Versão da política 4739
Documento da política JSON 4739
Saiba mais 4748
NovaActServiceRolePolicy 4748
Utilização desta política 4748
Detalhes desta política 4748
Versão da política 4748
Documento da política JSON 4749
Saiba mais 4749
OAMFullAccess 4749
Utilização desta política 4749
Detalhes desta política 4750
Versão da política 4750
Documento da política JSON 4750
Saiba mais 4750
OAMReadOnlyAccess 4751
Utilização desta política 4751
Detalhes desta política 4751
Versão da política 4751
Documento da política JSON 4751
Saiba mais 4752
OpensearchIngestionSelfManagedVpcePolicy 4752
Utilização desta política 4752
Detalhes desta política 4752
Versão da política 4752
Documento da política JSON 4753
Saiba mais 4753
PartnerCentralAccountManagementUserRoleAssociation 4753
Utilização desta política 4754
Detalhes desta política 4754
Versão da política 4754
Documento da política JSON 4754
Saiba mais 4755

PartnerCentralIncentiveBenefitManagement 4755
Utilização desta política 4755
Detalhes desta política 4755
Versão da política 4756
Documento da política JSON 4756
Saiba mais 4760
PowerUserAccess 4760
Utilização desta política 4760
Detalhes desta política 4760
Versão da política 4760
Documento da política JSON 4760
Saiba mais 4761
PricingPlanManagerFullAccess 4761
Utilização desta política 4762
Detalhes desta política 4762
Versão da política 4762
Documento da política JSON 4762
Saiba mais 4763
PricingPlanManagerReadonlyAccess 4763
Utilização desta política 4763
Detalhes desta política 4763
Versão da política 4763
Documento da política JSON 4764
Saiba mais 4764
QAppsServiceRolePolicy 4764
Utilização desta política 4764
Detalhes desta política 4765
Versão da política 4765
Documento da política JSON 4765
Saiba mais 4765
QBusinessQuicksightPluginPolicy 4766
Utilização desta política 4766
Detalhes desta política 4766
Versão da política 4766
Documento da política JSON 4766
Saiba mais 4767

QBusinessServiceRolePolicy 4767
Utilização desta política 4767
Detalhes desta política 4767
Versão da política 4768
Documento da política JSON 4768
Saiba mais 4769
QuickSightAccessForS3StorageManagementAnalyticsReadOnly 4769
Utilização desta política 4770
Detalhes desta política 4770
Versão da política 4770
Documento da política JSON 4770
Saiba mais 4771
RDSCloudHsmAuthorizationRole 4771
Utilização desta política 4771
Detalhes desta política 4771
Versão da política 4771
Documento da política JSON 4772
Saiba mais 4772
ReadOnlyAccess 4772
Utilização desta política 4773
Detalhes desta política 4773
Versão da política 4773
Documento da política JSON 4773
Saiba mais 4842
ReInventTicketApprovalAccess 4843
Utilização desta política 4843
Detalhes desta política 4843
Versão da política 4843
Documento da política JSON 4843
Saiba mais 4844
ResourceGroupsandTagEditorFullAccess 4844
Utilização desta política 4844
Detalhes desta política 4844
Versão da política 4844
Documento da política JSON 4845
Saiba mais 4845

ResourceGroupsandTagEditorReadOnlyAccess 4845
Utilização desta política 4846
Detalhes desta política 4846
Versão da política 4846
Documento da política JSON 4846
Saiba mais 4847
ResourceGroupsServiceRolePolicy 4847
Utilização desta política 4847
Detalhes desta política 4847
Versão da política 4847
Documento da política JSON 4848
Saiba mais 4848
ResourceGroupsTaggingAPITagUntagSupportedResources 4848
Utilização desta política 4848
Detalhes desta política 4849
Versão da política 4849
Documento da política JSON 4849
Saiba mais 4857
ROSAAmazonEBSCSIDriverOperatorPolicy 4857
Utilização desta política 4858
Detalhes desta política 4858
Versão da política 4858
Documento da política JSON 4858
Saiba mais 4866
ROSACloudNetworkConfigOperatorPolicy 4866
Utilização desta política 4867
Detalhes desta política 4867
Versão da política 4867
Documento da política JSON 4867
Saiba mais 4868
ROSAControlPlaneOperatorPolicy 4868
Utilização desta política 4868
Detalhes desta política 4868
Versão da política 4869
Documento da política JSON 4869
Saiba mais 4874

ROSAImageRegistryOperatorPolicy 4874
Utilização desta política 4874
Detalhes desta política 4874
Versão da política 4875
Documento da política JSON 4875
Saiba mais 4876
ROSAIngressOperatorPolicy 4876
Utilização desta política 4876
Detalhes desta política 4877
Versão da política 4877
Documento da política JSON 4877
Saiba mais 4878
ROSAInstallerPolicy 4878
Utilização desta política 4878
Detalhes desta política 4878
Versão da política 4878
Documento da política JSON 4879
Saiba mais 4887
ROSAKarpenterControllerPolicy 4887
Utilização desta política 4887
Detalhes desta política 4888
Versão da política 4888
Documento da política JSON 4888
Saiba mais 4894
ROSAKMSProviderPolicy 4895
Utilização desta política 4895
Detalhes desta política 4895
Versão da política 4895
Documento da política JSON 4895
Saiba mais 4896
ROSAKubeControllerPolicy 4896
Utilização desta política 4896
Detalhes desta política 4896
Versão da política 4897
Documento da política JSON 4897
Saiba mais 4901

ROSAManageSubscription 4902
Utilização desta política 4902
Detalhes desta política 4902
Versão da política 4902
Documento da política JSON 4902
Saiba mais 4903
ROSANodePoolManagementPolicy 4903
Utilização desta política 4904
Detalhes desta política 4904
Versão da política 4904
Documento da política JSON 4904
Saiba mais 4910
ROSASharedVPCEndpointPolicy 4911
Utilização desta política 4911
Detalhes desta política 4911
Versão da política 4911
Documento da política JSON 4911
Saiba mais 4915
ROSASharedVPCRoute53Policy 4915
Utilização desta política 4915
Detalhes desta política 4916
Versão da política 4916
Documento da política JSON 4916
Saiba mais 4917
ROSASRESupportPolicy 4917
Utilização desta política 4918
Detalhes desta política 4918
Versão da política 4918
Documento da política JSON 4918
Saiba mais 4923
ROSAWorkerInstancePolicy 4923
Utilização desta política 4923
Detalhes desta política 4923
Versão da política 4924
Documento da política JSON 4924
Saiba mais 4925

Route53RecoveryReadinessServiceRolePolicy 4925
Utilização desta política 4925
Detalhes desta política 4925
Versão da política 4926
Documento da política JSON 4926
Saiba mais 4929
Route53ResolverServiceRolePolicy 4929
Utilização desta política 4930
Detalhes desta política 4930
Versão da política 4930
Documento da política JSON 4930
Saiba mais 4931
RTBFabricServiceRolePolicy 4931
Utilização desta política 4931
Detalhes desta política 4931
Versão da política 4931
Documento da política JSON 4932
Saiba mais 4934
S3StorageLensServiceRolePolicy 4934
Utilização desta política 4934
Detalhes desta política 4934
Versão da política 4934
Documento da política JSON 4935
Saiba mais 4935
SageMakerStudioAdminIAMConsolePolicy 4935
Utilização desta política 4936
Detalhes desta política 4936
Versão da política 4936
Documento da política JSON 4936
Saiba mais 4948
SageMakerStudioAdminIAMDefaultExecutionPolicy 4948
Utilização desta política 4949
Detalhes desta política 4949
Versão da política 4949
Documento da política JSON 4949
Saiba mais 4974

SageMakerStudioAdminIAMPermissiveExecutionPolicy 4975
Utilização desta política 4975
Detalhes desta política 4975
Versão da política 4975
Documento da política JSON 4975
Saiba mais 4994
SageMakerStudioAdminProjectUserRolePolicy 4994
Utilização desta política 4994
Detalhes desta política 4995
Versão da política 4995
Documento da política JSON 4995
Saiba mais 4997
SageMakerStudioBedrockAgentServiceRolePolicy 4998
Utilização desta política 4998
Detalhes desta política 4998
Versão da política 4998
Documento da política JSON 4998
Saiba mais 5002
SageMakerStudioBedrockChatAgentUserRolePolicy 5002
Utilização desta política 5002
Detalhes desta política 5002
Versão da política 5002
Documento da política JSON 5003
Saiba mais 5007
SageMakerStudioBedrockEvaluationJobServiceRolePolicy 5007
Utilização desta política 5007
Detalhes desta política 5007
Versão da política 5007
Documento da política JSON 5008
Saiba mais 5011
SageMakerStudioBedrockFlowServiceRolePolicy 5011
Utilização desta política 5012
Detalhes desta política 5012
Versão da política 5012
Documento da política JSON 5012
Saiba mais 5016

SageMakerStudioBedrockFunctionExecutionRolePolicy 5016
Utilização desta política 5016
Detalhes desta política 5016
Versão da política 5017
Documento da política JSON 5017
Saiba mais 5018
SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy 5018
Utilização desta política 5018
Detalhes desta política 5018
Versão da política 5019
Documento da política JSON 5019
Saiba mais 5020
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy 5020
Utilização desta política 5020
Detalhes desta política 5020
Versão da política 5020
Documento da política JSON 5021
Saiba mais 5026
SageMakerStudioBedrockPromptUserRolePolicy 5026
Utilização desta política 5027
Detalhes desta política 5027
Versão da política 5027
Documento da política JSON 5027
Saiba mais 5029
SageMakerStudioDomainExecutionRolePolicy 5030
Utilização desta política 5030
Detalhes desta política 5030
Versão da política 5030
Documento da política JSON 5030
Saiba mais 5037
SageMakerStudioDomainServiceRolePolicy 5037
Utilização desta política 5037
Detalhes desta política 5037
Versão da política 5037
Documento da política JSON 5038
Saiba mais 5039

SageMakerStudioEMRContainersSystemNamespaceRolePolicy 5039
Utilização desta política 5039
Detalhes desta política 5039
Versão da política 5039
Documento da política JSON 5040
Saiba mais 5041
SageMakerStudioEMRInstanceRolePolicy 5041
Utilização desta política 5042
Detalhes desta política 5042
Versão da política 5042
Documento da política JSON 5042
Saiba mais 5046
SageMakerStudioEMRServiceRolePolicy 5046
Utilização desta política 5046
Detalhes desta política 5046
Versão da política 5046
Documento da política JSON 5047
Saiba mais 5049
SageMakerStudioFullAccess 5049
Utilização desta política 5049
Detalhes desta política 5049
Versão da política 5049
Documento da política JSON 5050
Saiba mais 5060
SageMakerStudioProjectProvisioningRolePolicy 5060
Utilização desta política 5060
Detalhes desta política 5060
Versão da política 5060
Documento da política JSON 5061
Saiba mais 5130
SageMakerStudioProjectRoleMachineLearningPolicy 5130
Utilização desta política 5130
Detalhes desta política 5130
Versão da política 5131
Documento da política JSON 5131
Saiba mais 5161

SageMakerStudioProjectUserRolePermissionsBoundary 5161
Utilização desta política 5162
Detalhes desta política 5162
Versão da política 5162
Documento da política JSON 5162
Saiba mais 5217
SageMakerStudioProjectUserRolePolicy 5218
Utilização desta política 5218
Detalhes desta política 5218
Versão da política 5218
Documento da política JSON 5218
Saiba mais 5284
SageMakerStudioQueryExecutionRolePolicy 5284
Utilização desta política 5285
Detalhes desta política 5285
Versão da política 5285
Documento da política JSON 5285
Saiba mais 5287
SageMakerStudioUserIAMConsolePolicy 5287
Utilização desta política 5287
Detalhes desta política 5287
Versão da política 5288
Documento da política JSON 5288
Saiba mais 5289
SageMakerStudioUserIAMDefaultExecutionPolicy 5290
Utilização desta política 5290
Detalhes desta política 5290
Versão da política 5290
Documento da política JSON 5290
Saiba mais 5315
SageMakerStudioUserIAMPermissiveExecutionPolicy 5315
Utilização desta política 5315
Detalhes desta política 5315
Versão da política 5316
Documento da política JSON 5316
Saiba mais 5330

SecretsManagerReadWrite 5331
Utilização desta política 5331
Detalhes desta política 5331
Versão da política 5331
Documento da política JSON 5331
Saiba mais 5333
SecurityAgentWebAppAPIPolicy 5333
Utilização desta política 5334
Detalhes desta política 5334
Versão da política 5334
Documento da política JSON 5334
Saiba mais 5336
SecurityAgentWebAppPolicy 5336
Utilização desta política 5336
Detalhes desta política 5336
Versão da política 5336
Documento da política JSON 5337
Saiba mais 5338
SecurityAudit 5338
Utilização desta política 5339
Detalhes desta política 5339
Versão da política 5339
Documento da política JSON 5339
Saiba mais 5368
SecurityLakeResourceManagementServiceRolePolicy 5368
Utilização desta política 5368
Detalhes desta política 5368
Versão da política 5369
Documento da política JSON 5369
Saiba mais 5374
SecurityLakeServiceLinkedRole 5374
Utilização desta política 5375
Detalhes desta política 5375
Versão da política 5375
Documento da política JSON 5375
Saiba mais 5378

ServerMigration_ServiceRole 5378
Utilização desta política 5379
Detalhes desta política 5379
Versão da política 5379
Documento da política JSON 5379
Saiba mais 5384
ServerMigrationConnector 5384
Utilização desta política 5384
Detalhes desta política 5384
Versão da política 5385
Documento da política JSON 5385
Saiba mais 5386
ServerMigrationServiceConsoleFullAccess 5386
Utilização desta política 5387
Detalhes desta política 5387
Versão da política 5387
Documento da política JSON 5387
Saiba mais 5389
ServerMigrationServiceLaunchRole 5389
Utilização desta política 5389
Detalhes desta política 5389
Versão da política 5389
Documento da política JSON 5390
Saiba mais 5392
ServerMigrationServiceRoleForInstanceValidation 5392
Utilização desta política 5393
Detalhes desta política 5393
Versão da política 5393
Documento da política JSON 5393
Saiba mais 5394
ServiceQuotasFullAccess 5394
Utilização desta política 5394
Detalhes desta política 5394
Versão da política 5394
Documento da política JSON 5394
Saiba mais 5396

ServiceQuotasReadOnlyAccess 5396
Utilização desta política 5396
Detalhes desta política 5397
Versão da política 5397
Documento da política JSON 5397
Saiba mais 5398
ServiceQuotasServiceRolePolicy 5399
Utilização desta política 5399
Detalhes desta política 5399
Versão da política 5399
Documento da política JSON 5399
Saiba mais 5400
SignInLocalDevelopmentAccess 5400
Utilização desta política 5400
Detalhes desta política 5400
Versão da política 5400
Documento da política JSON 5401
Saiba mais 5401
SimpleWorkflowFullAccess 5401
Utilização desta política 5401
Detalhes desta política 5401
Versão da política 5402
Documento da política JSON 5402
Saiba mais 5402
SMSVoiceServiceRolePolicy 5402
Utilização desta política 5403
Detalhes desta política 5403
Versão da política 5403
Documento da política JSON 5403
Saiba mais 5404
SplitCostAllocationDataServiceRolePolicy 5404
Utilização desta política 5404
Detalhes desta política 5404
Versão da política 5404
Documento da política JSON 5405
Saiba mais 5405

SSMQuickSetupRolePolicy 5405
Utilização desta política 5406
Detalhes desta política 5406
Versão da política 5406
Documento da política JSON 5406
Saiba mais 5409
SupportUser 5409
Utilização desta política 5409
Detalhes desta política 5409
Versão da política 5410
Documento da política JSON 5410
Saiba mais 5415
SystemAdministrator 5415
Utilização desta política 5415
Detalhes desta política 5415
Versão da política 5416
Documento da política JSON 5416
Saiba mais 5422
TranslateFullAccess 5422
Utilização desta política 5422
Detalhes desta política 5422
Versão da política 5423
Documento da política JSON 5423
Saiba mais 5423
TranslateReadOnly 5424
Utilização desta política 5424
Detalhes desta política 5424
Versão da política 5424
Documento da política JSON 5424
Saiba mais 5425
ViewOnlyAccess 5425
Utilização desta política 5425
Detalhes desta política 5425
Versão da política 5425
Documento da política JSON 5426
Saiba mais 5443

VMImportExportRoleForAWSConnector 5443
Utilização desta política 5443
Detalhes desta política 5444
Versão da política 5444
Documento da política JSON 5444
Saiba mais 5445
VPCLatticeFullAccess 5445
Utilização desta política 5445
Detalhes desta política 5445
Versão da política 5445
Documento da política JSON 5446
Saiba mais 5448
VPCLatticeReadOnlyAccess 5448
Utilização desta política 5448
Detalhes desta política 5448
Versão da política 5448
Documento da política JSON 5448
Saiba mais 5449
VPCLatticeServicesInvokeAccess 5450
Utilização desta política 5450
Detalhes desta política 5450
Versão da política 5450
Documento da política JSON 5450
Saiba mais 5451
WAFLoggingServiceRolePolicy 5451
Utilização desta política 5451
Detalhes desta política 5451
Versão da política 5451
Documento da política JSON 5452
Saiba mais 5452
WAFRegionalLoggingServiceRolePolicy 5452
Utilização desta política 5453
Detalhes desta política 5453
Versão da política 5453
Documento da política JSON 5453
Saiba mais 5454

WAFV2LoggingServiceRolePolicy 5454
Utilização desta política 5454
Detalhes desta política 5454
Versão da política 5455
Documento da política JSON 5455
Saiba mais 5456
WellArchitectedAgentResourceScanning 5456
Utilização desta política 5456
Detalhes desta política 5456
Versão da política 5456
Documento da política JSON 5457
Saiba mais 5483
WellArchitectedConsoleFullAccess 5483
Utilização desta política 5483
Detalhes desta política 5483
Versão da política 5483
Documento da política JSON 5484
Saiba mais 5486
WellArchitectedConsoleReadOnlyAccess 5486
Utilização desta política 5487
Detalhes desta política 5487
Versão da política 5487
Documento da política JSON 5487
Saiba mais 5488
WorkLinkServiceRolePolicy 5488
Utilização desta política 5488
Detalhes desta política 5488
Versão da política 5488
Documento da política JSON 5489
Saiba mais 5489
..... 5490

O que são as políticas gerenciadas pela AWS?

Uma política gerenciada pela AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas pela AWS são projetadas para conceder permissões em muitos cenários de uso comum. Elas simplificam o processo de conceder permissões aos usuários, grupos e funções, comparados à elaboração manual de políticas.

Lembre-se de que as políticas gerenciadas pela AWS podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para uso por todos os clientes da AWS. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas em políticas gerenciadas pela AWS. Caso a AWS faça atualizações nas permissões estabelecidas em uma política gerenciada pela AWS, estas mudanças impactarão todas as identidades das entidades principais (usuários, grupos e funções) vinculadas à esta política. A AWS é mais propensa a atualizar uma política gerenciada pela AWS durante o lançamento de um novo serviço da AWS ou quando novas operações de API estiverem disponíveis para serviços existentes.

Para informações adicionais, consulte as Políticas Gerenciadas pela AWS na Guia do Usuário do IAM.

Compreender as páginas de referência de políticas

Cada página de referência de política fornece as seguintes informações:

- Utilização desta política: indica se é possível vincular esta política a usuários, grupos e funções
- Detalhes desta política
  - Tipo: o tipo de política gerenciada pela AWS
    - `AWS managed policy`: uma política padrão gerenciada pela AWS
    - `Job function policy` – Política alinhada com as funções comuns do setor
    - `Service-linked role policy` – Política que está vinculada a uma função associada a um serviço, possibilitando que um serviço execute ações em seu nome, tais como the section called “AmazonRDSPreviewServiceRolePolicy”
    - `Service role policy` – Política elaborada para ser compatível com funções de serviço, tais como the section called “AWSControlTowerServiceRolePolicy”

  - Horário de criação — Quando a política foi criada pela primeira vez
  - Hora da edição — Quando essa versão da política foi editada
  - ARN – O nome do recurso da Amazon (ARN) da política em questão
- Versão da política — A versão das permissões que foram concedidas pela política
- Documento da política JSON — A política JSON
- Saiba mais — Links para a documentação relacionada às políticas gerenciadas pela AWS

Políticas gerenciadas pela AWS obsoletas

A AWS atualiza regularmente as políticas gerenciadas pela AWS. Na maioria dos casos, incluímos permissões em uma política. Isto acontece quando lançamos um novo serviço ou atributo. Visando reforçar a segurança das políticas gerenciadas pela AWS, ocasionalmente restringimos o escopo dessas políticas. Ao remover as permissões de uma política, marcamos a política como obsoleta e disponibilizamos uma nova versão. No caso de a AWS descontinuar um serviço ou um atributo, também encerraremos a política gerenciada pela AWS associada a este recurso.

Se você receber um aviso por e-mail de que uma política que está utilizando tornou-se obsoleta, é altamente recomendado que tome medidas imediatamente. Identifique as alterações na política e atualize os seus fluxos de trabalho. Se a AWS oferecer uma política de substituição, planeje vinculá-la a todas as identidades afetadas (usuários, grupos e funções) e, posteriormente, desvincular a política obsoleta destas identidades.

Uma política obsoleta tem as seguintes características:

- Ela foi removida deste guia.
- Ela mantém as permissões operacionais para todas as identidades atualmente vinculadas.
- Nas contas em que a política está vinculada a uma identidade, ela é exibida na lista de Políticas no console do IAM com um ícone de aviso ao lado.
- Não é possível associá-la a nenhuma nova identidade. Se você desvinculá-la de uma identidade existente, não será possível reestabelecer esta conexão.
- Após desvinculá-la de todas as entidades atuais, ela deixará de ser visível.

AWS políticas gerenciadas

AWS políticas gerenciadas

- AccessAnalyzerServiceRolePolicy
- AccountAccessManagerServiceRolePolicy
- AccountManagementFromVercel
- AdministratorAccess
- AdministratorAccess-Amplify
- AdministratorAccess-AWSElasticBeanstalk
- AgentRegistryFullAccess
- AgentRegistryReadOnlyAccess
- AIDevOpsAgentAccessPolicy
- AIDevOpsAgentActionsPolicy
- AIDevOpsAgentFullAccess
- AIDevOpsAgentReadOnlyAccess
- AIDevOpsChannelAccessPolicy
- AIDevOpsConstellationAccessPolicy
- AIDevOpsOperatorAppAccessPolicy
- AIDevOpsReleaseManagementVPCPolicy
- AIOpsAssistantIncidentReportPolicy
- AIOpsAssistantPolicy
- AIOpsConsoleAdminPolicy
- AIOpsOperatorAccess
- AIOpsReadOnlyAccess
- AlexaForBusinessDeviceSetup
- AlexaForBusinessFullAccess
- AlexaForBusinessGatewayExecution
- AlexaForBusinessLifesizeDelegatedAccessPolicy
- AlexaForBusinessNetworkProfileServicePolicy

- AlexaForBusinessPolyDelegatedAccessPolicy
- AlexaForBusinessReadOnlyAccess
- AmazonAPIGatewayAdministrator
- AmazonAPIGatewayInvokeFullAccess
- AmazonAPIGatewayPushToCloudWatchLogs
- AmazonAppFlowFullAccess
- AmazonAppFlowReadOnlyAccess
- AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy
- AmazonAppStreamFullAccess
- AmazonAppStreamPCAAccess
- AmazonAppStreamReadOnlyAccess
- AmazonAppStreamServiceAccess
- AmazonAthenaFullAccess
- AmazonAthenaServiceRolePolicy
- AmazonAugmentedAIFullAccess
- AmazonAugmentedAIHumanLoopFullAccess
- AmazonAugmentedAIIntegratedAPIAccess
- AmazonAuroraDSQLConsoleFullAccess
- AmazonAuroraDSQLFullAccess
- AmazonAuroraDSQLReadOnlyAccess
- AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy
- AmazonBedrockExternalWebSearchFullAccess
- AmazonBedrockExternalWebSearchReadOnly
- AmazonBedrockFullAccess
- AmazonBedrockLimitedAccess
- AmazonBedrockMantleFullAccess
- AmazonBedrockMantleInferenceAccess
- AmazonBedrockMantleReadOnly
- AmazonBedrockMarketplaceAccess

- AmazonBedrockReadOnly
- AmazonBedrockStudioPermissionsBoundary
- AmazonBedrockWebSearchFullAccess
- AmazonBedrockWebSearchReadOnly
- AmazonBioDiscoveryFullAccess
- AmazonBioDiscoveryInAppFullAccess
- AmazonBraketFullAccess
- AmazonBraketJobsExecutionPolicy
- AmazonBraketServiceRolePolicy
- AmazonChimeFullAccess
- AmazonChimeReadOnly
- AmazonChimeSDK
- AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy
- AmazonChimeSDKMessagingServiceRolePolicy
- AmazonChimeServiceRolePolicy
- AmazonChimeTranscriptionServiceLinkedRolePolicy
- AmazonChimeUserManagement
- AmazonChimeVoiceConnectorServiceLinkedRolePolicy
- AmazonCloudDirectoryFullAccess
- AmazonCloudDirectoryReadOnlyAccess
- AmazonCloudWatchEvidentlyFullAccess
- AmazonCloudWatchEvidentlyReadOnlyAccess
- AmazonCloudWatchEvidentlyServiceRolePolicy
- AmazonCloudWatchRUMFullAccess
- AmazonCloudWatchRUMReadOnlyAccess
- AmazonCloudWatchRUMServiceRolePolicy
- AmazonCodeCatalystFullAccess
- AmazonCodeCatalystReadOnlyAccess
- AmazonCodeCatalystSupportAccess

- AmazonCodeGuruProfilerAgentAccess
- AmazonCodeGuruProfilerFullAccess
- AmazonCodeGuruProfilerReadOnlyAccess
- AmazonCodeGuruReviewerFullAccess
- AmazonCodeGuruReviewerReadOnlyAccess
- AmazonCodeGuruReviewerServiceRolePolicy
- AmazonCodeGuruSecurityFullAccess
- AmazonCodeGuruSecurityScanAccess
- AmazonCognitoDeveloperAuthenticatedIdentities
- AmazonCognitoIdpEmailServiceRolePolicy
- AmazonCognitoIdpServiceRolePolicy
- AmazonCognitoPowerUser
- AmazonCognitoReadOnly
- AmazonCognitoUnAuthedIdentitiesSessionPolicy
- AmazonCognitoUnauthenticatedIdentities
- AmazonConnect_FullAccess
- AmazonConnectCampaignsServiceLinkedRolePolicy
- AmazonConnectReadOnlyAccess
- AmazonConnectServiceLinkedRolePolicy
- AmazonConnectSynchronizationServiceRolePolicy
- AmazonConnectVoiceIDFullAccess
- AmazonDataZoneBedrockModelConsumptionPolicy
- AmazonDataZoneBedrockModelManagementPolicy
- AmazonDataZoneDomainExecutionRolePolicy
- AmazonDataZoneEnvironmentRolePermissionsBoundary
- AmazonDataZoneFullAccess
- AmazonDataZoneFullUserAccess
- AmazonDataZoneGlueManageAccessRolePolicy
- AmazonDataZonePortalFullAccessPolicy

- AmazonDataZonePreviewConsoleFullAccess
- AmazonDataZoneProjectDeploymentPermissionsBoundary
- AmazonDataZoneProjectRolePermissionsBoundary
- AmazonDataZoneRedshiftGlueProvisioningPolicy
- AmazonDataZoneRedshiftManageAccessRolePolicy
- AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary
- AmazonDataZoneSageMakerManageAccessRolePolicy
- AmazonDataZoneSageMakerProvisioningRolePolicy
- AmazonDetectiveFullAccess
- AmazonDetectiveInvestigatorAccess
- AmazonDetectiveMemberAccess
- AmazonDetectiveOrganizationsAccess
- AmazonDetectiveServiceLinkedRolePolicy
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruOrganizationsAccess
- AmazonDevOpsGuruReadOnlyAccess
- AmazonDevOpsGuruServiceRolePolicy
- AmazonDMSCloudWatchLogsRole
- AmazonDMSRedshiftS3Role
- AmazonDMSVPCManagementRole
- AmazonDocDB-ElasticServiceRolePolicy
- AmazonDocDBConsoleFullAccess
- AmazonDocDBElasticFullAccess
- AmazonDocDBElasticReadOnlyAccess
- AmazonDocDBFullAccess
- AmazonDocDBReadOnlyAccess
- Gerenciamento de RSVPC do Amazon
- AmazonDynamoDBFullAccess

- AmazonDynamoDBFullAccess_v2
- AmazonDynamoDBFullAccesswithDataPipeline
- AmazonDynamoDBReadOnlyAccess
- AmazonEBSCSIDriverEKSClusterScopedPolicy
- AmazonEBSCSIDriverPolicy
- AmazonEBSCSIDriverPolicyV2
- AmazonEC2ContainerRegistryFullAccess
- AmazonEC2ContainerRegistryPowerUser
- AmazonEC2ContainerRegistryPullOnly
- AmazonEC2ContainerRegistryReadOnly
- AmazonEC2ContainerServiceAutoscaleRole
- AmazonEC2ContainerServiceEventsRole
- AmazonEC2ContainerServiceforEC2Role
- AmazonEC2ContainerServiceRole
- AmazonEC2FullAccess
- AmazonEC2ImageReferencesAccessPolicy
- AmazonEC2ReadOnlyAccess
- AmazonEC2RoleforAWSCodeDeploy
- AmazonEC2RoleforAWSCodeDeployLimited
- AmazonEC2RoleforDataPipelineRole
- Função do Amazon EC2 para SSM
- AmazonEC2RolePolicyForLaunchWizard
- AmazonEC2SpotFleetAutoscaleRole
- AmazonEC2SpotFleetTaggingRole
- Amazon ECS_ FullAccess
- AmazonECSComputeServiceRolePolicy
- AmazonECSInfrastructureRoleforExpressGatewayServices
- AmazonECSInfrastructureRoleForGatewayHostSharedALB
- AmazonECSInfrastructureRolePolicyForLoadBalancers

- AmazonECSInfrastructureRolePolicyForManagedInstances
- AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity
- AmazonECSInfrastructureRolePolicyForVolumes
- AmazonECSInfrastructureRolePolicyForVpcLattice
- AmazonECSInstanceRolePolicyForManagedInstances
- AmazonECSServiceRolePolicy
- AmazonECSTaskExecutionRolePolicy
- AmazonEFSCSIDriverPolicy
- AmazonEKS_CNI_Policy
- AmazonEKSBlockStoragePolicy
- AmazonEKSBlockStoragePolicyV2
- AmazonEKSClusterPolicy
- AmazonEKSComputePolicy
- AmazonEKSConnectorServiceRolePolicy
- AmazonEKSDashboardConsoleReadOnly
- AmazonEKSDashboardServiceRolePolicy
- AmazonEKSFargatePodExecutionRolePolicy
- AmazonEKSForFargateServiceRolePolicy
- AmazonEKSLoadBalancingPolicy
- AmazonEKSLocalOutpostClusterPolicy
- AmazonEKSLocalOutpostServiceRolePolicy
- AmazonEKSMCPReadOnlyAccess
- AmazonEKSNetworkingPolicy
- AmazonEKSServicePolicy
- AmazonEKSServiceRolePolicy
- AmazonEKSVPCResourceController
- AmazonEKSWorkerNodeMinimalPolicy
- AmazonEKSWorkerNodePolicy
- AmazonElastiCacheFullAccess

- AmazonElastiCacheReadOnlyAccess
- AmazonElasticContainerRegistryPublicFullAccess
- AmazonElasticContainerRegistryPublicPowerUser
- AmazonElasticContainerRegistryPublicReadOnly
- AmazonElasticFileSystemClientFullAccess
- AmazonElasticFileSystemClientReadOnlyAccess
- AmazonElasticFileSystemClientReadWriteAccess
- AmazonElasticFileSystemFullAccess
- AmazonElasticFileSystemReadOnlyAccess
- AmazonElasticFileSystemServiceRolePolicy
- AmazonElasticFileSystemsUtils
- AmazonElasticMapReduceEditorsRole
- AmazonElasticMapReduceforAutoScalingRole
- AmazonElasticMapReduceforEC2Role
- AmazonElasticMapReduceFullAccess
- AmazonElasticMapReducePlacementGroupPolicy
- AmazonElasticMapReduceReadOnlyAccess
- AmazonElasticMapReduceRole
- AmazonElasticsearchServiceRolePolicy
- AmazonElasticTranscoder_FullAccess
- AmazonElasticTranscoder_JobsSubmitter
- AmazonElasticTranscoder_ReadOnlyAccess
- AmazonElasticTranscoderRole
- AmazonEMRCleanupPolicy
- AmazonEMRContainersServiceRolePolicy
- AmazonEMRFullAccessPolicy_v2
- AmazonEMRReadOnlyAccessPolicy_v2
- AmazonEMRServerlessServiceRolePolicy
- AmazonEMRServicePolicy_v2

- AmazonEMRServicePolicyForSessions
- AmazonESCognitoAccess
- AmazonESFullAccess
- AmazonESReadOnlyAccess
- AmazonEventBridgeApiDestinationsServiceRolePolicy
- AmazonEventBridgeFullAccess
- AmazonEventBridgePipesFullAccess
- AmazonEventBridgePipesOperatorAccess
- AmazonEventBridgePipesReadOnlyAccess
- AmazonEventBridgeReadOnlyAccess
- AmazonEventBridgeSchedulerFullAccess
- AmazonEventBridgeSchedulerReadOnlyAccess
- AmazonEventBridgeSchemasFullAccess
- AmazonEventBridgeSchemasReadOnlyAccess
- AmazonEventBridgeSchemasServiceRolePolicy
- AmazonEVSServiceRolePolicy
- AmazonFISServiceRolePolicy
- AmazonForecastFullAccess
- AmazonFraudDetectorFullAccessPolicy
- AmazonFreeRTOSFullAccess
- AmazonFreeRTOSOTAUpdate
- AmazonFSxConsoleFullAccess
- AmazonFSxConsoleReadOnlyAccess
- AmazonFSxFullAccess
- AmazonFSxReadOnlyAccess
- AmazonFSxServiceRolePolicy
- AmazonGlacierFullAccess
- AmazonGlacierReadOnlyAccess
- AmazonGrafanaAthenaAccess

- AmazonGrafanaCloudWatchAccess
- AmazonGrafanaRedshiftAccess
- AmazonGrafanaServiceLinkedRolePolicy
- AmazonGuardDutyFullAccess
- AmazonGuardDutyFullAccess_v2
- AmazonGuardDutyMalwareProtectionServiceRolePolicy
- AmazonGuardDutyReadOnlyAccess
- AmazonGuardDutyServiceRolePolicy
- AmazonHealthLakeFullAccess
- AmazonHealthLakeReadOnlyAccess
- AmazonHoneycodeFullAccess
- AmazonHoneycodeReadOnlyAccess
- AmazonHoneycodeServiceRolePolicy
- AmazonHoneycodeTeamAssociationFullAccess
- AmazonHoneycodeTeamAssociationReadOnlyAccess
- AmazonHoneycodeWorkbookFullAccess
- AmazonHoneycodeWorkbookReadOnlyAccess
- AmazonInspector2AgentlessServiceRolePolicy
- AmazonInspector2AmiScanServiceRolePolicy
- AmazonInspector2FullAccess
- AmazonInspector2FullAccess_v2
- AmazonInspector2ManagedCisPolicy
- AmazonInspector2ManagedTelemetryPolicy
- AmazonInspector2ReadOnlyAccess
- AmazonInspector2ServiceRolePolicy
- AmazonInspector2ThirdPartyServiceRolePolicy
- AmazonInspectorFullAccess
- AmazonInspectorReadOnlyAccess
- AmazonInspectorServiceRolePolicy

- AmazonKendraFullAccess
- AmazonKendraReadOnlyAccess
- AmazonKeyspacesFullAccess
- AmazonKeyspacesReadOnlyAccess
- AmazonKeyspacesReadOnlyAccess_v2
- AmazonKinesisAnalyticsFullAccess
- AmazonKinesisAnalyticsReadOnly
- AmazonKinesisFirehoseFullAccess
- AmazonKinesisFirehoseReadOnlyAccess
- AmazonKinesisFullAccess
- AmazonKinesisReadOnlyAccess
- AmazonKinesisVideoStreamsFullAccess
- AmazonKinesisVideoStreamsReadOnlyAccess
- AmazonLaunchWizard_Acesso total
- AmazonLaunchWizardFullAccessV2
- AmazonLexChannelsAccess
- AmazonLexFullAccess
- AmazonLexReadOnly
- AmazonLexReplicationPolicy
- AmazonLexRunBotsOnly
- AmazonLexV2BotPolicy
- AmazonLookoutEquipmentFullAccess
- AmazonLookoutEquipmentReadOnlyAccess
- AmazonLookoutMetricsFullAccess
- AmazonLookoutMetricsReadOnlyAccess
- AmazonLookoutVisionConsoleFullAccess
- AmazonLookoutVisionConsoleReadOnlyAccess
- AmazonLookoutVisionFullAccess
- AmazonLookoutVisionReadOnlyAccess

- AmazonMachineLearningBatchPredictionsAccess
- AmazonMachineLearningCreateOnlyAccess
- AmazonMachineLearningFullAccess
- AmazonMachineLearningManageRealTimeEndpointOnlyAccess
- AmazonMachineLearningReadOnlyAccess
- AmazonMachineLearningRealTimePredictionOnlyAccess
- AmazonMachineLearningRoleforRedshiftDataSourceV3
- AmazonMacieFullAccess
- AmazonMacieHandshakeRole
- AmazonMacieReadOnlyAccess
- AmazonMacieServiceRole
- AmazonMacieServiceRolePolicy
- AmazonManagedBlockchainConsoleFullAccess
- AmazonManagedBlockchainFullAccess
- AmazonManagedBlockchainReadOnlyAccess
- AmazonManagedBlockchainServiceRolePolicy
- AmazonMCSFullAccess
- AmazonMCSReadOnlyAccess
- AmazonMechanicalTurkFullAccess
- AmazonMechanicalTurkReadOnly
- AmazonMemoryDBFullAccess
- AmazonMemoryDBReadOnlyAccess
- AmazonMobileAnalyticsFinancialReportAccess
- AmazonMobileAnalyticsFullAccess
- AmazonMobileAnalyticsNon-financialReportAccess
- AmazonMobileAnalyticsWriteOnlyAccess
- AmazonMonitronFullAccess
- AmazonMQApiFullAccess
- AmazonMQApiReadOnlyAccess

- AmazonMQFullAccess
- AmazonMQReadOnlyAccess
- AmazonMQServiceRolePolicy
- AmazonMSKConnectReadOnlyAccess
- AmazonMSKFullAccess
- AmazonMSKReadOnlyAccess
- AmazonMWAAServerlessServiceRolePolicy
- AmazonMWAAServiceRolePolicy
- AmazonNimbleStudio-LaunchProfileWorker
- AmazonNimbleStudio-StudioAdmin
- AmazonNimbleStudio-StudioUser
- AmazonODBAutonomousDatabaseAdmin
- AmazonODBAutonomousVmClusterAdmin
- AmazonODBExadataInfrastructureAdmin
- AmazonODBExadataVmClusterAdmin
- AmazonODBExascaleStorageVaultAdmin
- AmazonODBExascaleVmClusterAdmin
- AmazonODBFullAccess
- AmazonODBNetworkAdmin
- AmazonODBReadOnlyAccess
- AmazonODBServiceRolePolicy
- AmazonOmicsFullAccess
- AmazonOmicsReadOnlyAccess
- AmazonOneEnterpriseFullAccess
- AmazonOneEnterpriseInstallerAccess
- AmazonOneEnterpriseReadOnlyAccess
- AmazonOpenSearchDashboardsServiceRolePolicy
- AmazonOpenSearchDirectQueryGlueCreateAccess
- AmazonOpenSearchIngestionFullAccess

- AmazonOpenSearchIngestionReadOnlyAccess
- AmazonOpenSearchIngestionServiceRolePolicy
- AmazonOpenSearchServerlessServiceRolePolicy
- AmazonOpenSearchServiceCognitoAccess
- AmazonOpenSearchServiceFullAccess
- AmazonOpenSearchServiceReadOnlyAccess
- AmazonOpenSearchServiceRolePolicy
- AmazonPersonalizeFullAccess
- AmazonPollyFullAccess
- AmazonPollyReadOnlyAccess
- AmazonPrometheusConsoleFullAccess
- AmazonPrometheusFullAccess
- AmazonPrometheusQueryAccess
- AmazonPrometheusRemoteWriteAccess
- AmazonPrometheusScraperServiceRolePolicy
- AmazonQDeveloperAccess
- AmazonQFullAccess
- AmazonQLDBConsoleFullAccess
- AmazonQLDBFullAccess
- AmazonQLDBReadOnly
- AmazonRDSBetaServiceRolePolicy
- AmazonRDSCustomInstanceProfileRolePolicy
- AmazonRDSCustomPreviewServiceRolePolicy
- AmazonRDSCustomServiceRolePolicy
- AmazonRDSDataFullAccess
- AmazonRDSDirectoryServiceAccess
- AmazonRDSEnhancedMonitoringRole
- AmazonRDSFullAccess
- AmazonRDSPerformanceInsightsFullAccess

- AmazonRDSPerformanceInsightsReadOnly
- AmazonRDSPreviewServiceRolePolicy
- AmazonRDSReadOnlyAccess
- AmazonRDSServiceRolePolicy
- AmazonRedshiftAllCommandsFullAccess
- AmazonRedshiftDataFullAccess
- AmazonRedshiftFederatedAuthorization
- AmazonRedshiftFullAccess
- AmazonRedshiftQueryEditor
- AmazonRedshiftQueryEditorV2FullAccess
- AmazonRedshiftQueryEditorV2NoSharing
- AmazonRedshiftQueryEditorV2ReadSharing
- AmazonRedshiftQueryEditorV2ReadWriteSharing
- AmazonRedshiftReadOnlyAccess
- AmazonRedshiftServiceLinkedRolePolicy
- AmazonRekognitionCustomLabelsFullAccess
- AmazonRekognitionFullAccess
- AmazonRekognitionReadOnlyAccess
- AmazonRekognitionServiceRole
- AmazonRoute53AutoNamingFullAccess
- AmazonRoute53AutoNamingReadOnlyAccess
- AmazonRoute53AutoNamingRegistrantAccess
- AmazonRoute53DomainsFullAccess
- AmazonRoute53DomainsReadOnlyAccess
- AmazonRoute53FullAccess
- AmazonRoute53GlobalResolverFullAccess
- AmazonRoute53GlobalResolverReadOnlyAccess
- AmazonRoute53ProfilesFullAccess
- AmazonRoute53ProfilesReadOnlyAccess

- AmazonRoute53ReadOnlyAccess
- AmazonRoute53RecoveryClusterFullAccess
- AmazonRoute53RecoveryClusterReadOnlyAccess
- AmazonRoute53RecoveryControlConfigFullAccess
- AmazonRoute53RecoveryControlConfigReadOnlyAccess
- AmazonRoute53RecoveryReadinessFullAccess
- AmazonRoute53RecoveryReadinessReadOnlyAccess
- AmazonRoute53ResolverFullAccess
- AmazonRoute53ResolverReadOnlyAccess
- AmazonS3ExpressFullAccess
- AmazonS3ExpressReadOnlyAccess
- AmazonS3FilesClientFullAccess
- AmazonS3FilesClientReadOnlyAccess
- AmazonS3FilesClientReadWriteAccess
- AmazonS3FilesCSIDriverPolicy
- AmazonS3FilesFullAccess
- AmazonS3FilesReadOnlyAccess
- AmazonS3FullAccess
- AmazonS3ObjectLambdaExecutionRolePolicy
- AmazonS3OutpostsFullAccess
- AmazonS3OutpostsReadOnlyAccess
- AmazonS3ReadOnlyAccess
- AmazonS3TablesFullAccess
- AmazonS3TablesLakeFormationServiceRole
- AmazonS3TablesReadOnlyAccess
- AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy
- AmazonSageMakerCanvasAIServicesAccess
- AmazonSageMakerCanvasBedrockAccess
- AmazonSageMakerCanvasDataPrepFullAccess

- AmazonSageMakerCanvasDirectDeployAccess
- AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy
- AmazonSageMakerCanvasForecastAccess
- AmazonSageMakerCanvasFullAccess
- AmazonSageMakerCanvasSMDataScienceAssistantAccess
- AmazonSageMakerCapacityReservationServiceRolePolicy
- AmazonSageMakerClusterInstanceRolePolicy
- AmazonSageMakerCoreServiceRolePolicy
- AmazonSageMakerEdgeDeviceFleetPolicy
- AmazonSageMakerFeatureStoreAccess
- AmazonSageMakerFullAccess
- AmazonSageMakerGeospatialExecutionRole
- AmazonSageMakerGeospatialFullAccess
- AmazonSageMakerGroundTruthExecution
- AmazonSageMakerHyperPodGatedModelAccess
- AmazonSageMakerHyperPodInferenceAccess
- AmazonSageMakerHyperPodInferenceGatewayAccess
- AmazonSageMakerHyperPodObservabilityAdminAccess
- AmazonSageMakerHyperPodServiceRolePolicy
- AmazonSageMakerHyperPodTrainingOperatorAccess
- AmazonSageMakerInferenceServiceRolePolicy
- AmazonSageMakerJobFullAccess
- AmazonSageMakerJobRuntimeAccess
- AmazonSageMakerMechanicalTurkAccess
- AmazonSageMakerModelCustomizationCoreAccess
- AmazonSageMakerModelGovernanceUseAccess
- AmazonSageMakerModelRegistryFullAccess
- AmazonSageMakerNotebooksServiceRolePolicy
- AmazonSageMakerPartnerAppsFullAccess

- AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSageMakerPipelinesIntegrations
- AmazonSageMakerQuickSightVPCPolicy
- AmazonSageMakerReadOnly
- AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSageMakerSpacesControllerPolicy
- AmazonSageMakerSpacesRouterPolicy
- AmazonSageMakerTrainingPlanCreateAccess
- AmazonSecurityLakeAdministrator
- AmazonSecurityLakeMetastoreManager
- AmazonSecurityLakePermissionsBoundary
- AmazonSESFullAccess
- AmazonSESReadOnlyAccess
- AmazonSESServiceRolePolicy
- AmazonSNSFullAccess
- AmazonSNSReadOnlyAccess
- Função do Amazon SNS
- AmazonSQSFullAccess
- AmazonSQSReadOnlyAccess
- AmazonSSMAutomationApproverAccess

- AmazonSSMAutomationRole
- AmazonSSMDirectoryServiceAccess
- AmazonSSMFullAccess
- AmazonSSMMaintenanceWindowRole
- AmazonSSMManagedEC2InstanceDefaultPolicy
- AmazonSSMManagedInstanceCore
- AmazonSSMPatchAssociation
- AmazonSSMReadOnlyAccess
- AmazonSSMServiceRolePolicy
- AmazonSumerianFullAccess
- AmazonTextractFullAccess
- AmazonTextractServiceRole
- AmazonTimestreamConsoleFullAccess
- AmazonTimestreamFullAccess
- AmazonTimestreamInfluxDBFullAccess
- AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess
- AmazonTimestreamInfluxDBServiceRolePolicy
- AmazonTimestreamReadOnlyAccess
- AmazonTranscribeFullAccess
- AmazonTranscribeReadOnlyAccess
- AmazonVerifiedPermissionsFullAccess
- AmazonVerifiedPermissionsReadOnlyAccess
- AmazonVPCCrossAccountNetworkInterfaceOperations
- AmazonVPCFullAccess
- AmazonVPCNetworkAccessAnalyzerFullAccessPolicy
- AmazonVPCReachabilityAnalyzerFullAccessPolicy
- AmazonVPCReachabilityAnalyzerPathComponentReadPolicy
- AmazonVPCReadOnlyAccess
- AmazonWorkDocsFullAccess

- AmazonWorkDocsReadOnlyAccess
- AmazonWorkMailEventsServiceRolePolicy
- AmazonWorkMailFullAccess
- AmazonWorkMailMessageFlowFullAccess
- AmazonWorkMailMessageFlowReadOnlyAccess
- AmazonWorkMailReadOnlyAccess
- AmazonWorkSpacesAdmin
- AmazonWorkSpacesApplicationManagerAdminAccess
- AmazonWorkspacesPCAAccess
- AmazonWorkSpacesPoolServiceAccess
- AmazonWorkSpacesSecureBrowserReadOnly
- AmazonWorkSpacesSelfServiceAccess
- AmazonWorkSpacesServiceAccess
- AmazonWorkSpacesThinClientFullAccess
- AmazonWorkSpacesThinClientMonitoringServiceRolePolicy
- AmazonWorkSpacesThinClientReadOnlyAccess
- AmazonWorkSpacesWebReadOnly
- AmazonWorkSpacesWebServiceRolePolicy
- AmazonZocaloFullAccess
- AmazonZocaloReadOnlyAccess
- AmplifyBackendDeployFullAccess
- AnthropicFullAccess
- AnthropicLimitedAccess
- AnthropicReadOnlyAccess
- AnthropicSelfHostedEnvironmentAccess
- APIGatewayServiceRolePolicy
- AppIntegrationsServiceLinkedRolePolicy
- ApplicationAutoScalingForAmazonAppStreamAccess
- ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

- AppRunnerNetworkingServiceRolePolicy
- AppRunnerServiceRolePolicy
- AppStudioServiceRolePolicy
- AssuranceServiceRolePolicy
- AuroraDsqlServiceLinkedRolePolicy
- AutoScalingConsoleFullAccess
- AutoScalingConsoleReadOnlyAccess
- AutoScalingFullAccess
- AutoScalingNotificationAccessRole
- AutoScalingReadOnlyAccess
- AutoScalingServiceRolePolicy
- AWS-SSM-Automation-DiagnosisBucketPolicy
- AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy
- AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy
- AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy
- AWS-SSM-RemediationAutomation-AdministrationRolePolicy
- AWS-SSM-RemediationAutomation-ExecutionRolePolicy
- AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy
- AWS_ ConfigRole
- AWSAccountActivityAccess
- AWSAccountManagementFullAccess
- AWSAccountManagementReadOnlyAccess
- AWSAccountSettingsManagementRole
- AWSAccountUsageReportAccess
- AWSAgentlessDiscoveryService
- AWSAgentRegistryServiceRolePolicy
- AWSAppConfigServiceRolePolicy
- AWSAppFabricFullAccess
- AWSAppFabricReadOnlyAccess

- AWSAppFabricServiceRolePolicy
- AWSApplicationAutoscalingAppStreamFleetPolicy
- AWSApplicationAutoscalingCassandraTablePolicy
- AWSApplicationAutoscalingComprehendEndpointPolicy
- AWSApplicationAutoScalingCustomResourcePolicy
- AWSApplicationAutoscalingDynamoDBTablePolicy
- AWSApplicationAutoscalingEC2SpotFleetRequestPolicy
- AWSApplicationAutoscalingECSServicePolicy
- AWSApplicationAutoscalingElastiCacheRGPolicy
- AWSApplicationAutoscalingEMRInstanceGroupPolicy
- AWSApplicationAutoscalingKafkaClusterPolicy
- AWSApplicationAutoscalingLambdaConcurrencyPolicy
- AWSApplicationAutoscalingNeptuneClusterPolicy
- AWSApplicationAutoscalingRDSClusterPolicy
- AWSApplicationAutoscalingSageMakerEndpointPolicy
- AWSApplicationAutoscalingWorkSpacesPoolPolicy
- AWSApplicationDiscoveryAgentAccess
- AWSApplicationDiscoveryAgentlessCollectorAccess
- AWSApplicationDiscoveryServiceFullAccess
- AWSApplicationMigrationAgentInstallationPolicy
- AWSApplicationMigrationAgentPolicy
- AWSApplicationMigrationAgentPolicy_v2
- AWSApplicationMigrationConversionServerPolicy
- AWSApplicationMigrationEC2Access
- AWSApplicationMigrationFSxProxyPolicy
- AWSApplicationMigrationFSxProxyVPCPolicy
- AWSApplicationMigrationFullAccess
- AWSApplicationMigrationMGHAccess
- AWSApplicationMigrationNetworkMigrationCustomResource

- AWSApplicationMigrationNetworkMigrationMultiAccount
- AWSApplicationMigrationReadOnlyAccess
- AWSApplicationMigrationReplicationServerPolicy
- AWSApplicationMigrationServiceEc2InstancePolicy
- AWSApplicationMigrationServiceRolePolicy
- AWSApplicationMigrationSSMAccess
- AWSApplicationMigrationVCenterClientPolicy
- AWSAppMeshEnvoyAccess
- AWSAppMeshFullAccess
- AWSAppMeshPreviewEnvoyAccess
- AWSAppMeshPreviewServiceRolePolicy
- AWSAppMeshReadOnly
- AWSAppMeshServiceRolePolicy
- AWSAppRunnerFullAccess
- AWSAppRunnerReadOnlyAccess
- AWSAppRunnerServicePolicyForECRAccess
- AWSAppSyncAdministrator
- AWSAppSyncInvokeFullAccess
- AWSAppSyncPushToCloudWatchLogs
- AWSAppSyncSchemaAuthor
- AWSAppSyncServiceRolePolicy
- AWSArtifactAccountSync
- AWSArtifactAgreementsFullAccess
- AWSArtifactAgreementsReadOnlyAccess
- AWSArtifactComplianceInquiriesFullAccess
- AWSArtifactComplianceInquiriesReadOnlyAccess
- AWSArtifactReportsReadOnlyAccess
- AWSArtifactServiceRolePolicy
- AWSAuditManagerAdministratorAccess

- AWSAuditManagerServiceRolePolicy
- AWSAutoScalingPlansEC2AutoScalingPolicy
- AWSBackupAccessPointOperatorAccess
- AWSBackupAuditAccess
- AWSBackupDataTransferAccess
- AWSBackupFullAccess
- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync
- AWSBackupGuardDutyRolePolicyForScans
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupSearchOperatorAccess
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForIndexing
- AWSBackupServiceRolePolicyForItemRestores
- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSBackupServiceRolePolicyForScans
- AWSBatchFullAccess
- AWSBatchServiceEventTargetRole
- AWSBatchServiceRole
- AWSBatchServiceRolePolicyForSageMaker
- AWSBCMDataExportsServiceRolePolicy
- AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy
- AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy
- AWSBedrockAgentCoreRuntimeInstancesServiceRolePolicy

- AWSBillingConductorFullAccess
- AWSBillingConductorReadOnlyAccess
- AWSBillingConductorRolePolicy
- AWSBillingReadOnlyAccess
- AWSBillingServiceRolePolicy
- AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM
- AWSBudgetsActionsWithAWSResourceControlAccess
- AWSBudgetsReadOnlyAccess
- AWSBudgetsSpendLimitMemberRolePolicy
- AWSBugBustFullAccess
- AWSBugBustPlayerAccess
- AWSBugBustServiceRolePolicy
- AWSCertificateManagerFullAccess
- AWSCertificateManagerPrivateCAAuditor
- AWSCertificateManagerPrivateCAFullAccess
- AWSCertificateManagerPrivateCAPrivilegedUser
- AWSCertificateManagerPrivateCAReadOnly
- AWSCertificateManagerPrivateCAUser
- AWSCertificateManagerReadOnly
- AWSChatbotServiceLinkedRolePolicy
- AWSCleanRoomsFullAccess
- AWSCleanRoomsFullAccessNoQuerying
- AWSCleanRoomsMLFullAccess
- AWSCleanRoomsMLReadOnlyAccess
- AWSCleanRoomsReadOnlyAccess
- AWSCleanRoomsServiceRolePolicy
- AWSCloud9Administrator
- AWSCloud9EnvironmentMember
- AWSCloud9ServiceRolePolicy

- AWSCloud9SSMInstanceProfile
- AWSCloud9User
- AWSCloudFormationFullAccess
- AWSCloudFormationReadOnlyAccess
- AWSCloudFrontLogger
- AWSCloudFrontVPCOriginServiceRolePolicy
- AWSCloudHSMFullAccess
- AWSCloudHSMReadOnlyAccess
- AWSCloudHSMRole
- AWSCloudMapDiscoverInstanceAccess
- AWSCloudMapFullAccess
- AWSCloudMapReadOnlyAccess
- AWSCloudMapRegisterInstanceAccess
- AWSCloudShellFullAccess
- AWSCloudTrail_FullAccess
- AWSCloudTrail_ReadOnlyAccess
- AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy
- AWSCloudWatchOmniServiceRolePolicy
- AWSCodeArtifactAdminAccess
- AWSCodeArtifactReadOnlyAccess
- AWSCodeBuildAdminAccess
- AWSCodeBuildDeveloperAccess
- AWSCodeBuildReadOnlyAccess
- AWSCodeCommitFullAccess
- AWSCodeCommitPowerUser
- AWSCodeCommitReadOnly
- AWSCodeDeployDeployerAccess
- AWSCodeDeployFullAccess
- AWSCodeDeployReadOnlyAccess

- AWSCodeDeployRole
- AWSCodeDeployRoleForCloudFormation
- AWSCodeDeployRoleForECS
- AWSCodeDeployRoleForECSLimited
- AWSCodeDeployRoleForLambda
- AWSCodeDeployRoleForLambdaLimited
- AWSCodePipeline_FullAccess
- AWSCodePipeline_ReadOnlyAccess
- AWSCodePipelineApproverAccess
- AWSCodePipelineCustomActionAccess
- AWSCodeStarFullAccess
- AWSCodeStarNotificationsServiceRolePolicy
- AWSCodeStarServiceRole
- AWSCompromisedKeyQuarantine
- AWSCompromisedKeyQuarantineV2
- AWSCompromisedKeyQuarantineV3
- AWSConfigMultiAccountSetupPolicy
- AWSConfigRemediationServiceRolePolicy
- AWSConfigRoleForOrganizations
- AWSConfigRulesExecutionRole
- AWSConfigServiceRolePolicy
- AWSConfigThirdPartyServiceRolePolicy
- AWSConfigUserAccess
- Conector AWS
- AWSControlTowerAccountServiceRolePolicy
- AWSControlTowerCloudTrailRolePolicy
- AWSControlTowerIdentityCenterManagementPolicy
- AWSControlTowerServiceRolePolicy
- AWSCostAndUsageReportAutomationPolicy

- AWSDataExchangeDataGrantOwnerFullAccess
- AWSDataExchangeDataGrantReceiverFullAccess
- AWSDataExchangeFullAccess
- AWSDataExchangeProviderFullAccess
- AWSDataExchangeReadOnly
- AWSDataExchangeServiceRolePolicyForLicenseManagement
- AWSDataExchangeServiceRolePolicyForOrganizationDiscovery
- AWSDataExchangeSubscriberFullAccess
- AWSDataLifecycleManagerServiceRole
- AWSDataLifecycleManagerServiceRoleForAMIManagement
- AWSDataLifecycleManagerSSMFullAccess
- AWSDataPipeline_FullAccess
- AWSDataPipeline_PowerUser
- AWSDataSyncDiscoveryServiceRolePolicy
- AWSDataSyncFullAccess
- AWSDataSyncReadOnlyAccess
- AWSDataSyncServiceRolePolicy
- AWSDeadlineCloud-FleetWorker
- AWSDeadlineCloud-UserAccessFarms
- AWSDeadlineCloud-UserAccessFleets
- AWSDeadlineCloud-UserAccessJobs
- AWSDeadlineCloud-UserAccessQueues
- AWSDeadlineCloud-WorkerHost
- AWSDeepLensLambdaFunctionAccessPolicy
- AWSDeepLensServiceRolePolicy
- AWSDeepRacerAccountAdminAccess
- AWSDeepRacerCloudFormationAccessPolicy
- AWSDeepRacerDefaultMultiUserAccess
- AWSDeepRacerFullAccess
- AWSDeepRacerRoboMakerAccessPolicy

- AWSDeepRacerServiceRolePolicy
- AWSDenyAll
- AWSDeviceFarmFullAccess
- AWSDeviceFarmServiceRolePolicy
- AWSDeviceFarmTestGridServiceRolePolicy
- AWSDirectConnectFullAccess
- AWSDirectConnectReadOnlyAccess
- AWSDirectConnectServiceRolePolicy
- AWSDirectoryServiceDataFullAccess
- AWSDirectoryServiceDataReadOnlyAccess
- AWSDirectoryServiceFullAccess
- AWSDirectoryServiceReadOnlyAccess
- AWSDirectoryServiceServiceRolePolicy
- AWSDiscoveryContinuousExportFirehosePolicy
- AWSDMSFleetAdvisorServiceRolePolicy
- AWSDMSServerlessServiceRolePolicy
- AWSEC2CapacityManagerServiceRolePolicy
- AWSEC2CapacityReservationFleetRolePolicy
- AWSEC2FleetServiceRolePolicy
- AWSEC2SpotFleetServiceRolePolicy
- AWSEC2SpotServiceRolePolicy
- AWSEC2SqlHaInstancePolicy
- AWSEC2SqlHaServiceRolePolicy
- AWSEC2VssRestorePolicy
- AWSEC2VssSnapshotPolicy
- AWSECRPullThroughCache_ServiceRolePolicy
- AWSElasticBeanstalkCustomPlatformforEC2Role
- AWSElasticBeanstalkEKSImageBuild
- AWSElasticBeanstalkEKSObservability
- AWSElasticBeanstalkEKSTagging

- AWSElasticBeanstalkEnhancedHealth
- AWSElasticBeanstalkMaintenance
- AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy
- AWSElasticBeanstalkManagedUpdatesServiceRolePolicy
- AWSElasticBeanstalkMulticontainerDocker
- AWSElasticBeanstalkReadOnly
- AWSElasticBeanstalkRoleCore
- AWSElasticBeanstalkRoleCWL
- AWSElasticBeanstalkRoleECS
- AWSElasticBeanstalkRoleRDS
- AWSElasticBeanstalkRoleSNS
- AWSElasticBeanstalkRoleWorkerTier
- AWSElasticBeanstalkService
- AWSElasticBeanstalkServiceRolePolicy
- AWSElasticBeanstalkWebTier
- AWSElasticBeanstalkWorkerTier
- AWSElasticDisasterRecoveryAgentInstallationPolicy
- AWSElasticDisasterRecoveryAgentPolicy
- AWSElasticDisasterRecoveryConsoleFullAccess
- AWSElasticDisasterRecoveryConsoleFullAccess_v2
- AWSElasticDisasterRecoveryConversionServerPolicy
- AWSElasticDisasterRecoveryCrossAccountReplicationPolicy
- AWSElasticDisasterRecoveryEc2InstancePolicy
- AWSElasticDisasterRecoveryFailbackInstallationPolicy
- AWSElasticDisasterRecoveryFailbackPolicy
- AWSElasticDisasterRecoveryLaunchActionsPolicy
- AWSElasticDisasterRecoveryNetworkReplicationPolicy
- AWSElasticDisasterRecoveryReadOnlyAccess
- AWSElasticDisasterRecoveryRecoveryInstancePolicy
- AWSElasticDisasterRecoveryReplicationServerPolicy

- AWSElasticDisasterRecoveryServiceRolePolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy_v2
- AWSElasticLoadBalancingClassicServiceRolePolicy
- AWSElasticLoadBalancingServiceRolePolicy
- AWSElementalMediaConnectCreateBridge
- AWSElementalMediaConnectCreateFlow
- AWSElementalMediaConnectDeleteBridge
- AWSElementalMediaConnectDeleteFlow
- AWSElementalMediaConnectFullAccess
- AWSElementalMediaConnectReadOnlyAccess
- AWSElementalMediaConvertFullAccess
- AWSElementalMediaConvertReadOnly
- AWSElementalMediaLiveFullAccess
- AWSElementalMediaLiveReadOnly
- AWSElementalMediaPackageFullAccess
- AWSElementalMediaPackageReadOnly
- AWSElementalMediaPackageV2FullAccess
- AWSElementalMediaPackageV2ReadOnly
- AWSElementalMediaStoreFullAccess
- AWSElementalMediaStoreReadOnly
- AWSElementalMediaTailorFullAccess
- AWSElementalMediaTailorReadOnly
- AWSEnhancedClassicNetworkingMangementPolicy
- AWSEntityResolutionConsoleFullAccess
- AWSEntityResolutionConsoleReadOnlyAccess
- AWSFaultInjectionSimulatorEC2Access
- AWSFaultInjectionSimulatorECSAccess
- AWSFaultInjectionSimulatorEKSAccess
- AWSFaultInjectionSimulatorNetworkAccess

- AWSFaultInjectionSimulatorRDSAccess
- AWSFaultInjectionSimulatorSSMAccess
- AWSFinSpaceServiceRolePolicy
- AWSFMAdminFullAccess
- AWSFMAdminReadOnlyAccess
- AWSFMMemberReadOnlyAccess
- AWSForWordPressPluginPolicy
- AWSGitSyncServiceRolePolicy
- AWSGlobalAcceleratorSLRPolicy
- AWSGlueConsoleFullAccess
- AWSGlueConsoleSageMakerNotebookFullAccess
- AwsGlueDataBrewFullAccessPolicy
- AWSGlueDataBrewServiceRole
- AWSGlueSchemaRegistryFullAccess
- AWSGlueSchemaRegistryReadonlyAccess
- AWSGlueServiceNotebookRole
- AWSGlueServiceRole
- AwsGlueSessionUserRestrictedNotebookPolicy
- AwsGlueSessionUserRestrictedNotebookServiceRole
- AwsGlueSessionUserRestrictedPolicy
- AwsGlueSessionUserRestrictedServiceRole
- AWSGrafanaAccountAdministrator
- AWSGrafanaConsoleReadOnlyAccess
- AWSGrafanaWorkspacePermissionManagement
- AWSGrafanaWorkspacePermissionManagementV2
- AWSGreengrassFullAccess
- AWSGreengrassReadOnlyAccess
- AWSGreengrassResourceAccessRolePolicy
- AWSGroundStationAgentInstancePolicy
- AWS Health_EventProcessorServiceRolePolicy

- AWSHealthFullAccess
- AWSHealthImagingFullAccess
- AWSHealthImagingReadOnlyAccess
- AWSHealthImagingServiceRolePolicy
- AWSHealthOmicsServiceLinkedRolePolicy
- AWSIAMIdentityCenterAllowListForIdentityContext
- AWSIAMRoleManagerServiceRolePolicy
- AWSIdentityCenterExternalManagementPolicy
- AWSIdentitySyncFullAccess
- AWSIdentitySyncReadOnlyAccess
- AWSImageBuilderFullAccess
- AWSImageBuilderReadOnlyAccess
- AWSImportExportFullAccess
- AWSImportExportReadOnlyAccess
- AWSIncidentManagerIncidentAccessServiceRolePolicy
- AWSIncidentManagerResolverAccess
- AWSIncidentManagerServiceRolePolicy
- AWSIoT1ClickFullAccess
- AWSIoT1ClickReadOnlyAccess
- AWSIoTAnalyticsFullAccess
- AWSIoTAnalyticsReadOnlyAccess
- AWSIoTConfigAccess
- AWSIoTConfigReadOnlyAccess
- AWSIoTDataAccess
- AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction
- AWSIoTDeviceDefenderAudit
- AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction
- AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction
- AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction
- AWSIoTDeviceDefenderUpdateCACertMitigationAction

- AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction
- AWSIoTDeviceTesterForFreeRTOSFullAccess
- AWSIoTDeviceTesterForGreengrassFullAccess
- AWSIoTEventsFullAccess
- AWSIoTEventsReadOnlyAccess
- AWSIoTFleetHubFederationAccess
- AWSIoTFleetwiseServiceRolePolicy
- AWSIoTFullAccess
- AWSIoTLogging
- AWSIoTManagedIntegrationsFullAccess
- AWSIoTManagedIntegrationsRolePolicy
- AWSIoTOTAUpdate
- AWSIotRoboRunnerFullAccess
- AWSIotRoboRunnerReadOnly
- AWSIotRoboRunnerServiceRolePolicy
- AWSIoTRuleActions
- AWSIoTSiteWiseConsoleFullAccess
- AWSIoTSiteWiseFullAccess
- AWSIoTSiteWiseMonitorPortalAccess
- AWSIoTSiteWiseMonitorServiceRolePolicy
- AWSIoTSiteWiseReadOnlyAccess
- AWSIoTThingsRegistration
- AWSIoTTwinMakerServiceRolePolicy
- AWSIoTWirelessDataAccess
- AWSIoTWirelessFullAccess
- AWSIoTWirelessFullPublishAccess
- AWSIoTWirelessGatewayCertManager
- AWSIoTWirelessLogging
- AWSIoTWirelessReadOnlyAccess
- AWSIPAMServiceRolePolicy

- AWSIQContractServiceRolePolicy
- AWSIQFullAccess
- AWSIQPermissionServiceRolePolicy
- AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy
- AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy
- AWSKeyManagementServicePowerUser
- AWSLakeFormationCrossAccountManager
- AWSLakeFormationDataAdmin
- AWS Lambda_FullAccess
- AWS Lambda_ReadOnlyAccess
- AWSLambdaBasicDurableExecutionRolePolicy
- AWSLambdaBasicExecutionRole
- AWSLambdaDynamoDBExecutionRole
- AWSLambdaENIManagementAccess
- AWSLambdaExecute
- AWSLambdaFullAccess
- AWSLambdaInvocation-DynamoDB
- AWSLambdaInvokeWebFunctionEndpointAccess
- AWSLambdaKinesisExecutionRole
- AWSLambdaManagedEC2ResourceOperator
- AWSLambdaMSKExecutionRole
- AWSLambdaNetworkConnectorOperatorPolicy
- AWSLambdaReplicator
- AWSLambdaRole
- AWSLambdaServiceRolePolicy
- AWSLambdaSQSQueueExecutionRole
- AWSLambdaVPCAccessExecutionRole
- AWSLicenseManagerConsumptionPolicy
- AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy
- AWSLicenseManagerMasterAccountRolePolicy

- AWSLicenseManagerMemberAccountRolePolicy
- AWSLicenseManagerServiceRolePolicy
- AWSLicenseManagerUserSubscriptionsServiceRolePolicy
- AWSM2ServicePolicy
- AWSManagedAccountManagementAccess
- AWSManagedAccountUserEntitlementAccess
- AWSManagedAdvancedFeaturesActivationAccess
- AWSManagedBudgetsSpendLimitManagementAccess
- AWSManagedControlPolicyManagementAccess
- AWSManagedServiceAccessManagementAccess
- AWSManagedServices_ContactsServiceRolePolicy
- AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy
- AWSManagedServices_EventsServiceRolePolicy
- AWSManagedServices_SelfServiceReporting_ServiceRolePolicy
- AWSManagedServicesDeploymentToolkitPolicy
- AWSManagedSettingsAdminAccess
- AWSManagedSettingsReadOnlyAccess
- AWSManagedSignUpAdminAccess
- AWSManagementConsoleAdministratorAccess
- AWSManagementConsoleBasicUserAccess
- AWSMarketplaceAmiIngestion
- AWSMarketplaceDeploymentServiceRolePolicy
- AWSMarketplaceDiscoveryFullAccess
- AWSMarketplaceFullAccess
- AWSMarketplaceGetEntitlements
- AWSMarketplaceImageBuildFullAccess
- AWSMarketplaceLicenseManagementServiceRolePolicy
- AWSMarketplaceManageSubscriptions
- AWSMarketplaceMeteringFullAccess
- AWSMarketplaceMeteringRegisterUsage

- AWSMarketplaceProcurementSystemAdminFullAccess
- AWSMarketplacePurchaseOrdersServiceRolePolicy
- AWSMarketplaceRead-only
- AWSMarketplaceResaleAuthorizationServiceRolePolicy
- AWSMarketplaceSellerFullAccess
- AWSMarketplaceSellerOfferManagement
- AWSMarketplaceSellerProductsFullAccess
- AWSMarketplaceSellerProductsReadOnly
- AWSMcpServiceActionsFullAccess
- AWSMCPSignInOAuthAccessPolicy
- AWSMediaConnectServicePolicy
- AWSMediaLiveAnywhereServiceRolePolicy
- AWSMediaTailorServiceRolePolicy
- AWSMigrationHubDiscoveryAccess
- AWSMigrationHubDMSAccess
- AWSMigrationHubFullAccess
- AWSMigrationHubOrchestratorConsoleFullAccess
- AWSMigrationHubOrchestratorInstanceRolePolicy
- AWSMigrationHubOrchestratorPlugin
- AWSMigrationHubOrchestratorServiceRolePolicy
- AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess
- AWSMigrationHubRefactorSpaces-SSMAutomationPolicy
- AWSMigrationHubRefactorSpacesFullAccess
- AWSMigrationHubRefactorSpacesServiceRolePolicy
- AWSMigrationHubSMSAccess
- AWSMigrationHubStrategyCollector
- AWSMigrationHubStrategyConsoleFullAccess
- AWSMigrationHubStrategyServiceRolePolicy
- AWSMobileHub_FullAccess
- AWSMobileHub_ReadOnly

- AWSMSKReplicatorExecutionRole
- AWSNATGatewayServiceRolePolicy
- AWSNetworkFirewallFullAccess
- AWSNetworkFirewallReadOnlyAccess
- AWSNetworkFirewallServiceRolePolicy
- AWSNetworkManagerCloudWANServiceRolePolicy
- AWSNetworkManagerFullAccess
- AWSNetworkManagerReadOnlyAccess
- AWSNetworkManagerServiceRolePolicy
- AWSObservabilityAdminLogsCentralizationServiceRolePolicy
- AWSObservabilityAdminServiceRolePolicy
- AWSObservabilityAdminTelemetryEnablementServiceRolePolicy
- AWSOrganizationsFullAccess
- AWSOrganizationsReadOnlyAccess
- AWSOrganizationsServiceTrustPolicy
- AWSOutpostsAuthorizeServerPolicy
- AWSOutpostsServiceRolePolicy
- AWSPanoramaApplianceRolePolicy
- AWSPanoramaApplianceServiceRolePolicy
- AWSPanoramaFullAccess
- AWSPanoramaGreengrassGroupRolePolicy
- AWSPanoramaSageMakerRolePolicy
- AWSPanoramaServiceLinkedRolePolicy
- AWSPanoramaServiceRolePolicy
- AWSPartnerCentralChannelHandshakeApprovalManagement
- AWSPartnerCentralChannelManagement
- AWSPartnerCentralFullAccess
- AWSPartnerCentralMarketingManagement
- AWSPartnerCentralOpportunityManagement
- AWSPartnerCentralRevenueAttributionManagement

- AWSPartnerCentralSandboxFullAccess
- AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy
- AWSPartnerLedSupportReadOnlyAccess
- AWSPartnerProServeToolsFullAccess
- AWSPartnerProServeToolsIndividualContributor
- AWSPartnerProServeToolsOrganizationReaderIndividualContributor
- AWSPCSComputeNodePolicy
- AWSPCSServiceRolePolicy
- AWSPriceListServiceFullAccess
- AWSPrivateCAAuditor
- AWSPrivateCAConnectorForKubernetesPolicy
- AWSPrivateCAFullAccess
- AWSPrivateCAPrivilegedUser
- AWSPrivateCAReadOnly
- AWSPrivateCAUser
- AWSPrivateMarketplaceAdminFullAccess
- AWSPrivateMarketplaceRequests
- AWSPrivateNetworksServiceRolePolicy
- AWSProtonCodeBuildProvisioningBasicAccess
- AWSProtonCodeBuildProvisioningServiceRolePolicy
- AWSProtonDeveloperAccess
- AWSProtonFullAccess
- AWSProtonReadOnlyAccess
- AWSProtonServiceGitSyncServiceRolePolicy
- AWSProtonSyncServiceRolePolicy
- AWSPurchaseOrdersServiceRolePolicy
- AWSQuickSetupCFGCPacksPermissionsBoundary
- AWSQuickSetupDeploymentRolePolicy
- AWSQuickSetupDevOpsGuruPermissionsBoundary
- AWSQuickSetupDistributorPermissionsBoundary

- AWSQuickSetupEnableAREXExecutionPolicy
- AWSQuickSetupEnableDHMCExecutionPolicy
- AWSQuickSetupJITNADeploymentRolePolicy
- AWSQuickSetupManagedInstanceProfileExecutionPolicy
- AWSQuickSetupManageJITNAResourcesExecutionPolicy
- AWSQuickSetupPatchPolicyBaselineAccess
- AWSQuickSetupPatchPolicyDeploymentRolePolicy
- AWSQuickSetupPatchPolicyLambdaExecutionPolicy
- AWSQuickSetupPatchPolicyPermissionsBoundary
- AWSQuickSetupPatchPolicyTagManagementExecutionPolicy
- AWSQuickSetupSchedulerPermissionsBoundary
- AWSQuickSetupSSMDeploymentRolePolicy
- AWSQuickSetupSSMDeploymentS3BucketRolePolicy
- AWSQuickSetupSSMHostMgmtPermissionsBoundary
- AWSQuickSetupSSMLifecycleManagementExecutionPolicy
- AWSQuickSetupSSMManageResourcesExecutionPolicy
- AWSQuickSetupStartSSMAssociationsExecutionPolicy
- AWSQuickSetupStartStopInstancesExecutionPolicy
- AWSQuickSightAssetBundleExportPolicy
- AWSQuickSightAssetBundleImportPolicy
- AWSQuicksightAthenaAccess
- AWSQuickSightDescribeRDS
- AWSQuickSightDescribeRedshift
- AWSQuickSightElasticsearchPolicy
- AWSQuickSightIoTAnalyticsAccess
- AWSQuickSightListIAM
- AWSQuicksightOpenSearchPolicy
- AWSQuickSightSageMakerPolicy
- AWSQuickSightSecretsManagerWriteAccess
- AWSQuickSightSecretsManagerWritePolicy

- AWSQuickSightTimestreamPolicy
- AWSReachabilityAnalyzerServiceRolePolicy
- AWSRefactoringToolkitFullAccess
- AWSRefactoringToolkitSidecarPolicy
- AWSrePostPrivateCloudWatchAccess
- AWSRepostSpaceSupportOperationsPolicy
- AWSResilienceHubAsssessmentExecutionPolicy
- AWSResilienceHubResilienceTestingPolicy
- AWSResilienceHubServiceRolePolicy
- AWSResilienceHubV2AssessmentExecutionPolicy
- AWSResourceAccessManagerFullAccess
- AWSResourceAccessManagerReadOnlyAccess
- AWSResourceAccessManagerResourceShareParticipantAccess
- AWSResourceAccessManagerServiceRolePolicy
- AWSResourceExplorerFullAccess
- AWSResourceExplorerOrganizationsAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy
- AWSResourceGroupsReadOnlyAccess
- AWSRevenueAttributionManagement
- AWSRoboMaker_FullAccess
- AWSRoboMakerReadOnlyAccess
- AWSRoboMakerServicePolicy
- AWSRoboMakerServiceRolePolicy
- AWSRolesAnywhereFullAccess
- AWSRolesAnywhereReadOnly
- AWSRolesAnywhereServicePolicy
- AWSS3OnOutpostsServiceRolePolicy
- AWSSavingsPlansFullAccess
- AWSSavingsPlansReadOnlyAccess

- AWSSDMPServiceRolePolicy
- AWSSecretsManagerClientReadOnlyAccess
- AWSSecurityAgentServiceRolePolicy
- AWSSecurityAgentWebAppPolicy
- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess
- AWSSecurityHubReadOnlyAccess
- AWSSecurityHubServiceRolePolicy
- AWSSecurityHubV2ServiceRolePolicy
- AWSSecurityIncidentResponseCaseFullAccess
- AWSSecurityIncidentResponseFullAccess
- AWSSecurityIncidentResponseReadOnlyAccess
- AWSSecurityIncidentResponseServiceRolePolicy
- AWSSecurityIncidentResponseTriageServiceRolePolicy
- AWSServiceCatalogAdminFullAccess
- AWSServiceCatalogAdminReadOnlyAccess
- AWSServiceCatalogAppRegistryFullAccess
- AWSServiceCatalogAppRegistryReadOnlyAccess
- AWSServiceCatalogAppRegistryServiceRolePolicy
- AWSServiceCatalogEndUserFullAccess
- AWSServiceCatalogEndUserReadOnlyAccess
- AWSServiceCatalogOrgsDataSyncServiceRolePolicy
- AWSServiceCatalogSyncServiceRolePolicy
- AWSServiceRoleForAIDevOpsPolicy
- AWSServiceRoleForAmazonEKSNodegroup
- AWSServiceRoleForAmazonQDeveloper
- AWSServiceRoleForAWSTransform
- AWSServiceRoleForAWSTransformCustom
- AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy
- AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy

- AWSServiceRoleForCodeGuru-Profiler
- AWSServiceRoleForCodeWhispererPolicy
- AWSServiceRoleForEC2ScheduledInstances
- AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy
- AWSServiceRoleForImageBuilder
- AWSServiceRoleForIoTSiteWise
- AWSServiceRoleForLogDeliveryPolicy
- AWSServiceRoleForMonitronPolicy
- AWSServiceRoleForNeptuneGraphPolicy
- AWSServiceRoleForPrivateMarketplaceAdminPolicy
- AWSServiceRoleForProcurementInsightsPolicy
- AWSServiceRoleForSMS
- AWSServiceRoleForUserSubscriptions
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting
- AWSServiceRolePolicyForWorkspacesInstances
- AWSShieldDRTAccessPolicy
- AWSShieldServiceRolePolicy
- AWSSocialMessagingServiceRolePolicy
- AWSSSMForSAPServiceLinkedRolePolicy
- AWSSSMOpsInsightsServiceRolePolicy
- AWSSSODirectoryAdministrator
- AWSSSODirectoryReadOnly
- AWSSSOMasterAccountAdministrator
- AWSSSOMemberAccountAdministrator
- AWSSSOReadOnly
- AWSSSOServiceRolePolicy
- AWSStepFunctionsConsoleFullAccess
- AWSStepFunctionsFullAccess
- AWSStepFunctionsReadOnlyAccess

- AWSStorageGatewayFullAccess
- AWSStorageGatewayReadOnlyAccess
- AWSStorageGatewayServiceRolePolicy
- AWSSupplyChainFederationAdminAccess
- AWSSupportAccess
- AWSSupportAppFullAccess
- AWSSupportAppReadOnlyAccess
- AWSSupportPlansFullAccess
- AWSSupportPlansReadOnlyAccess
- AWSSupportPlansServiceRolePolicy
- AWSSupportServiceRolePolicy
- AWSSystemsManagerAccountDiscoveryServicePolicy
- AWSSystemsManagerChangeManagementServicePolicy
- AWSSystemsManagerEnableConfigRecordingExecutionPolicy
- AWSSystemsManagerEnableExplorerExecutionPolicy
- AWSSystemsManagerForSAPFullAccess
- AWSSystemsManagerForSAPReadOnlyAccess
- AWSSystemsManagerJustInTimeAccessServicePolicy
- AWSSystemsManagerJustInTimeAccessTokenPolicy
- AWSSystemsManagerJustInTimeAccessTokenSessionPolicy
- AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy
- AWSSystemsManagerNotificationsServicePolicy
- AWSSystemsManagerOpsDataSyncServiceRolePolicy
- AWSThinkboxAssetServerPolicy
- AWSThinkboxAWSPortalAdminPolicy
- AWSThinkboxAWSPortalGatewayPolicy
- AWSThinkboxAWSPortalWorkerPolicy
- AWSThinkboxDeadlineResourceTrackerAccessPolicy
- AWSThinkboxDeadlineResourceTrackerAdminPolicy
- AWSThinkboxDeadlineSpotEventPluginAdminPolicy

- AWSThinkboxDeadlineSpotEventPluginWorkerPolicy
- AWSTransferConsoleFullAccess
- AWSTransferFullAccess
- AWSTransferLoggingAccess
- AWSTransferReadOnlyAccess
- AWSTransferServiceRolePolicy
- AWSTransformApplicationDeploymentPolicy
- AWSTransformApplicationECSDeploymentPolicy
- AWSTransformCustomExecuteTransformations
- AWSTransformCustomFullAccess
- AWSTransformCustomManageTransformations
- AWSTransformInfrastructureExecutorAccessBatch
- AWSTransformInfrastructureExecutorAccessEC2
- AWSTransformLandingZoneAgentPolicy
- AWSTransformNetworkMigrationAgentPolicy
- AWSTransformRevenueAttributionPolicy
- AWSTransformSecretsManagerConnectorPolicy
- AWSTransformSecurityAgentExecutorAccess
- AWSTransformServerMigrationAgentPolicy
- AWSTrustedAdvisorPriorityFullAccess
- AWSTrustedAdvisorPriorityReadOnlyAccess
- AWSTrustedAdvisorReportingServiceRolePolicy
- AWSTrustedAdvisorServiceRolePolicy
- AWSUserAttributeCostAllocationPolicy
- AWSUserNotificationsServiceLinkedRolePolicy
- AWSVendorInsightsAssessorFullAccess
- AWSVendorInsightsAssessorReadOnly
- AWSVendorInsightsVendorFullAccess
- AWSVendorInsightsVendorReadOnly
- AWSVPCFlowLogsServiceRolePolicy

- AWSVpcLatticeServiceRolePolicy
- AWSVPCS2SVpnServiceRolePolicy
- AWSVPCTransitGatewayServiceRolePolicy
- AWSVPCVerifiedAccessServiceRolePolicy
- AWSWAFConsoleFullAccess
- AWSWAFConsoleReadOnlyAccess
- AWSWAFFullAccess
- AWSWAFReadOnlyAccess
- AWSWellArchitectedAgentOrganizationsServiceRolePolicy
- AWSWellArchitectedAgentResourceScanningServiceRolePolicy
- AWSWellArchitectedDiscoveryServiceRolePolicy
- AWSWellArchitectedOrganizationsServiceRolePolicy
- AWSWickrFullAccess
- AWSXrayCrossAccountSharingConfiguration
- AWSXRayDaemonWriteAccess
- AWSXrayFullAccess
- AWSXrayReadOnlyAccess
- AWSXrayWriteOnlyAccess
- AWSZonalAutoshiftPracticeRunSLRPolicy
- AWSZoneGroupAccessManagementServiceRolePolicy
- BatchServiceRolePolicy
- BedrockAgentCoreFullAccess
- BedrockAgentCoreNetworkServiceRolePolicy
- BedrockAgentCoreRuntimeIdentityServiceRolePolicy
- BedrockAgentCoreRuntimeInstancesInstanceRolePolicy
- BedrockAgentCoreRuntimeInstancesOperatorRolePolicy
- Faturamento
- BudgetsServiceRolePolicy
- CertificateManagerServiceRolePolicy
- ClientVPNServiceConnectionsRolePolicy

- ClientVPNServiceRolePolicy
- CloudFormationStackSetsOrgAdminServiceRolePolicy
- CloudFormationStackSetsOrgMemberServiceRolePolicy
- CloudFrontFullAccess
- CloudFrontReadOnlyAccess
- CloudHSMServiceRolePolicy
- CloudSearchFullAccess
- CloudSearchReadOnlyAccess
- CloudTrailEventContext
- CloudTrailServiceRolePolicy
- CloudWatch-CrossAccountAccess
- CloudWatchActionsEC2Access
- CloudWatchAgentAdminPolicy
- CloudWatchAgentServerPolicy
- CloudWatchAPIKeyAccess
- CloudWatchApplicationInsightsFullAccess
- CloudWatchApplicationInsightsReadOnlyAccess
- CloudwatchApplicationInsightsServiceLinkedRolePolicy
- CloudWatchApplicationSignalsFullAccess
- CloudWatchApplicationSignalsReadOnlyAccess
- CloudWatchApplicationSignalsServiceRolePolicy
- CloudWatchAutomaticDashboardsAccess
- CloudWatchCrossAccountSharingConfiguration
- CloudWatchEventsBuiltInTargetExecutionAccess
- CloudWatchEventsFullAccess
- CloudWatchEventsInvocationAccess
- CloudWatchEventsReadOnlyAccess
- CloudWatchEventsServiceRolePolicy
- CloudWatchFullAccess
- CloudWatchFullAccessV2

- CloudWatchInternetMonitorFullAccess
- CloudWatchInternetMonitorReadOnlyAccess
- CloudWatchInternetMonitorServiceRolePolicy
- CloudWatchLambdaApplicationSignalsExecutionRolePolicy
- CloudWatchLambdaInsightsExecutionRolePolicy
- CloudWatchLogsAPIKeyAccess
- CloudWatchLogsCrossAccountSharingConfiguration
- CloudWatchLogsFullAccess
- CloudWatchLogsReadOnlyAccess
- CloudWatchNetworkFlowMonitorAgentPublishPolicy
- CloudWatchNetworkFlowMonitorServiceRolePolicy
- CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy
- CloudWatchNetworkMonitorServiceRolePolicy
- CloudWatchOmniAWSIntegrationPolicy
- CloudWatchOmniDomainAccessPolicy
- CloudWatchOmniModelInferencePolicy
- CloudWatchOmniSpaceAccessPolicy
- CloudWatchOpenSearchDashboardAccess
- CloudWatchOpenSearchDashboardsFullAccess
- CloudWatchReadOnlyAccess
- CloudWatchSyntheticsFullAccess
- CloudWatchSyntheticsReadOnlyAccess
- ComprehendDataAccessRolePolicy
- ComprehendFullAccess
- ComprehendMedicalFullAccess
- ComprehendReadOnly
- ComputeOptimizerAutomationServiceRolePolicy
- ComputeOptimizerReadOnlyAccess
- ComputeOptimizerServiceRolePolicy
- ConfigConformsServiceRolePolicy

- ConsoleFullAccessFromVercel
- ConsoleViewOnlyAccessFromVercel
- CostOptimizationHubAdminAccess
- CostOptimizationHubReadOnlyAccess
- CostOptimizationHubServiceRolePolicy
- CustomerProfilesServiceLinkedRolePolicy
- DatabaseAdministrator
- DataScientist
- DAXServiceRolePolicy
- DBModDiscoveryAndAssessment
- DBModProvisioningAndMigration
- DBModVirtualSource
- DeclarativePoliciesEC2Report
- DynamoDBCloudWatchContributorInsightsServiceRolePolicy
- DynamoDBGlobalTableSettingsManagementServiceRolePolicy
- DynamoDBKinesisReplicationServiceRolePolicy
- DynamoDBReplicationServiceRolePolicy
- EC2ApplicationStatusChecksServiceRolePolicy
- EC2FastLaunchFullAccess
- EC2FastLaunchServiceRolePolicy
- EC2FleetTimeShiftableServiceRolePolicy
- Ec2ImageBuilderCrossAccountDistributionAccess
- EC2ImageBuilderExecutionPolicy
- EC2ImageBuilderLifecycleExecutionPolicy
- EC2InstanceConnect
- Ec2InstanceConnectEndpoint
- EC2InstanceProfileForImageBuilder
- EC2InstanceProfileForImageBuilderECRContainerBuilds
- ECRReplicationServiceRolePolicy
- ECRTemplateServiceRolePolicy

- ElastiCacheServiceRolePolicy
- ElasticLoadBalancingFullAccess
- ElasticLoadBalancingReadOnly
- ElementalActivationsDownloadSoftwareAccess
- ElementalActivationsFullAccess
- ElementalActivationsGenerateLicenses
- ElementalActivationsReadOnlyAccess
- ElementalAppliancesSoftwareFullAccess
- ElementalAppliancesSoftwareReadOnlyAccess
- ElementalSupportCenterFullAccess
- EMRDescribeClusterPolicyForEMRWAL
- EndUserMessagingServiceRolePolicy
- FinOpsAgentAgentPolicy
- FinOpsAgentOperatorPolicy
- FMSServiceRolePolicy
- FSxDeleteServiceLinkedRoleAccess
- GameLiftContainerFleetPolicy
- GameLiftGameServerGroupPolicy
- GitLabDuoWithAmazonQPermissionsPolicy
- GlobalAcceleratorFullAccess
- GlobalAcceleratorReadOnlyAccess
- GreengrassOTAUpdateArtifactAccess
- GroundTruthSyntheticConsoleFullAccess
- GroundTruthSyntheticConsoleReadOnlyAccess
- Health_OrganizationsServiceRolePolicy
- IAMAccessAdvisorReadOnly
- IAMAccessAnalyzerFullAccess
- IAMAccessAnalyzerReadOnlyAccess
- IAMFullAccess
- IAMReadOnlyAccess

- IAMSelfManageServiceSpecificCredentials
- IAMUserChangePassword
- IAMUserSSHKeys
- IVSFullAccess
- IVSReadOnlyAccess
- IVSRecordToS3
- KafkaConnectServiceRolePolicy
- KafkaServiceRolePolicy
- KeyspacesCDCServiceRolePolicy
- KeyspacesReplicationServiceRolePolicy
- LakeFormationDataAccessServiceRolePolicy
- LexBotPolicy
- LexChannelPolicy
- LightsailExportAccess
- MediaConnectGatewayInstanceRolePolicy
- MediaPackageServiceRolePolicy
- MemoryDBServiceRolePolicy
- MigrationHubDMSAccessServiceRolePolicy
- MigrationHubServiceRolePolicy
- MigrationHubSMSAccessServiceRolePolicy
- MonitronServiceRolePolicy
- MultiPartyApprovalFullAccess
- MultiPartyApprovalReadOnlyAccess
- NeptuneConsoleFullAccess
- NeptuneFullAccess
- NeptuneGraphReadOnlyAccess
- NeptuneReadOnlyAccess
- NetworkAdministrator
- NetworkSecurityDirectorServiceLinkedRolePolicy
- NetworkSecurityManagerServiceRolePolicy

- NovaActServiceRolePolicy
- OAMFullAccess
- OAMReadOnlyAccess
- OpensearchIngestionSelfManagedVpcePolicy
- PartnerCentralAccountManagementUserRoleAssociation
- PartnerCentralIncentiveBenefitManagement
- PowerUserAccess
- PricingPlanManagerFullAccess
- PricingPlanManagerReadonlyAccess
- QAppsServiceRolePolicy
- QBusinessQuicksightPluginPolicy
- QBusinessServiceRolePolicy
- QuickSightAccessForS3StorageManagementAnalyticsReadOnly
- RDSCloudHsmAuthorizationRole
- ReadOnlyAccess
- ReInventTicketApprovalAccess
- ResourceGroupsandTagEditorFullAccess
- ResourceGroupsandTagEditorReadOnlyAccess
- ResourceGroupsServiceRolePolicy
- ResourceGroupsTaggingAPITagUntagSupportedResources
- ROSAAmazonEBSCSIDriverOperatorPolicy
- ROSACloudNetworkConfigOperatorPolicy
- ROSAControlPlaneOperatorPolicy
- ROSAImageRegistryOperatorPolicy
- ROSAIngressOperatorPolicy
- ROSAInstallerPolicy
- ROSAKarpenterControllerPolicy
- ROSAKMSProviderPolicy
- ROSAKubeControllerPolicy
- ROSAManageSubscription

- ROSANodePoolManagementPolicy
- ROSASharedVPCEndpointPolicy
- ROSASharedVPCRoute53Policy
- ROSASRESupportPolicy
- ROSAWorkerInstancePolicy
- Route53RecoveryReadinessServiceRolePolicy
- Route53ResolverServiceRolePolicy
- RTBFabricServiceRolePolicy
- S3StorageLensServiceRolePolicy
- SageMakerStudioAdminIAMConsolePolicy
- SageMakerStudioAdminIAMDefaultExecutionPolicy
- SageMakerStudioAdminIAMPermissiveExecutionPolicy
- SageMakerStudioAdminProjectUserRolePolicy
- SageMakerStudioBedrockAgentServiceRolePolicy
- SageMakerStudioBedrockChatAgentUserRolePolicy
- SageMakerStudioBedrockEvaluationJobServiceRolePolicy
- SageMakerStudioBedrockFlowServiceRolePolicy
- SageMakerStudioBedrockFunctionExecutionRolePolicy
- SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy
- SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy
- SageMakerStudioBedrockPromptUserRolePolicy
- SageMakerStudioDomainExecutionRolePolicy
- SageMakerStudioDomainServiceRolePolicy
- SageMakerStudioEMRContainersSystemNamespaceRolePolicy
- SageMakerStudioEMRInstanceRolePolicy
- SageMakerStudioEMRServiceRolePolicy
- SageMakerStudioFullAccess
- SageMakerStudioProjectProvisioningRolePolicy
- SageMakerStudioProjectRoleMachineLearningPolicy
- SageMakerStudioProjectUserRolePermissionsBoundary

- SageMakerStudioProjectUserRolePolicy
- SageMakerStudioQueryExecutionRolePolicy
- SageMakerStudioUserIAMConsolePolicy
- SageMakerStudioUserIAMDefaultExecutionPolicy
- SageMakerStudioUserIAMPermissiveExecutionPolicy
- SecretsManagerReadWrite
- SecurityAgentWebAppAPIPolicy
- SecurityAgentWebAppPolicy
- SecurityAudit
- SecurityLakeResourceManagementServiceRolePolicy
- SecurityLakeServiceLinkedRole
- ServerMigration_ServiceRole
- ServerMigrationConnector
- ServerMigrationServiceConsoleFullAccess
- ServerMigrationServiceLaunchRole
- ServerMigrationServiceRoleForInstanceValidation
- ServiceQuotasFullAccess
- ServiceQuotasReadOnlyAccess
- ServiceQuotasServiceRolePolicy
- SignInLocalDevelopmentAccess
- SimpleWorkflowFullAccess
- SMSVoiceServiceRolePolicy
- SplitCostAllocationDataServiceRolePolicy
- SSMQuickSetupRolePolicy
- SupportUser
- SystemAdministrator
- TranslateFullAccess
- TranslateReadOnly
- ViewOnlyAccess
- VMImportExportRoleForAWSConnector

- VPCLatticeFullAccess
- VPCLatticeReadOnlyAccess
- VPCLatticeServicesInvokeAccess
- WAFLoggingServiceRolePolicy
- WAFRegionalLoggingServiceRolePolicy
- WAFV2LoggingServiceRolePolicy
- WellArchitectedAgentResourceScanning
- WellArchitectedConsoleFullAccess
- WellArchitectedConsoleReadOnlyAccess
- WorkLinkServiceRolePolicy

AccessAnalyzerServiceRolePolicy

Descrição: permitir que o Analisador de Acesso analise os metadados do recurso

`AccessAnalyzerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 02 de dezembro de 2019, 17:13 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

Versão da política

Versão da política: v23 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessAnalyzerServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ecr:DescribeRepositories",
        "ecr:GetAccountSetting",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "iam:GetRole",
        "iam:ListEntitiesForPolicy",
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListRoleTags",
        "iam:ListUserTags",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetUser",
        "iam:GetGroup",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetails",
        "iam:ListAccessKeys",
        "iam:GetLoginProfile",
        "iam:GetAccessKeyLastUsed",
```

```
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListUserPolicies",
        "iam:GetUserPolicy",
        "iam:ListAttachedUserPolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListGroupsForUser",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListVersionsByFunction",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "s3:DescribeMultiRegionAccessPointOperation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
```

```
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetBucketPolicy",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "sns:GetTopicAttributes",
        "sns:ListTopics",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AccountAccessManagerServiceRolePolicy

Descrição: Concede ao gerente de acesso à conta permissões para gerenciar o Conta da AWS acesso

`AccountAccessManagerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 29 de junho de 2026, 19:12 UTC
- Horário editado: 29 de junho de 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccountAccessManagerServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeAccount",
```

```
      "Resource" : "arn:aws:organizations::*:account/o-*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AccountManagementFromVercel

Descrição: Para uso com contas criadas por meio da integração do Vercel Marketplace com AWS. Fornece acesso ao gerenciamento de contas, notificação, análise de custo e uso e gerenciamento de provedores de identidade.

`AccountManagementFromVercel` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AccountManagementFromVercel` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 11 de dezembro de 2025, 16:34 UTC
- Horário editado: 07 de maio de 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AccountManagementFromVercel`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:CloseAccount",
        "bcm-recommended-actions:ListRecommendedActions",
        "ce:GetCostAndUsage",
        "cur:GetUsageReport",
        "iam:ListSAMLProviders",
        "freetier:GetFreeTierUsage",
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:UpdateSamlProvider",
        "iam:GetSamlProvider"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VercelInstallId" : "${aws:PrincipalTag/VercelInstallId}"
        }
      }
    },
    {
      "Sid" : "ManageServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy",
```

```
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Vercel/Service_2026_04_16",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VercelInstallId" : "${aws:PrincipalTag/VercelInstallId}",
          "iam:PermissionsBoundary" : [
            "arn:aws:iam::partner:policy/permissions-boundary/vercel.com/
VercelMarketplaceServiceRoleBoundary_2026_04_16"
          ]
        }
      }
    },
    {
      "Sid" : "TagManageServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Vercel/Service_2026_04_16",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/VercelInstallId" : "${aws:PrincipalTag/VercelInstallId}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AdministratorAccess

Descrição: Fornece acesso total aos AWS serviços e recursos.

`AdministratorAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AdministratorAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:39 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "*",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AdministratorAccess-Amplify

Descrição: concede permissões administrativas à conta e, ao mesmo tempo, autoriza explicitamente o acesso direto aos recursos essenciais para aplicações Amplify.

`AdministratorAccess-Amplify` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AdministratorAccess-Amplify` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2020, 19:03 UTC
- Hora da edição: 4 de abril de 2024, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CLICloudformationPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
```

```
        "cloudformation:DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackSet",
        "cloudformation:UpdateStackSet",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*"
      ]
    },
    {
      "Sid" : "CLIManageviaCFNPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoleTags",
        "iam:TagRole",
        "iam:AttachRolePolicy",
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePolicy",
        "iam:UntagRole",
        "iam:UpdateRole",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetRolePolicy",
        "iam:PassRole",
        "iam:ListPolicyVersions",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:CreateRole",
```

```
        "iam:ListRolePolicies",
        "iam:PutRolePermissionsBoundary",
        "iam:DeleteRolePermissionsBoundary",
        "appsync:CreateApiKey",
        "appsync:CreateDataSource",
        "appsync:CreateFunction",
        "appsync:CreateResolver",
        "appsync:CreateType",
        "appsync:DeleteApiKey",
        "appsync:DeleteDataSource",
        "appsync:DeleteFunction",
        "appsync:DeleteResolver",
        "appsync:DeleteType",
        "appsync:GetDataSource",
        "appsync:GetFunction",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResolver",
        "appsync:GetSchemaCreationStatus",
        "appsync:GetType",
        "appsync:GraphQL",
        "appsync:ListApiKeys",
        "appsync:ListDataSources",
        "appsync:ListFunctions",
        "appsync:ListGraphqlApis",
        "appsync:ListResolvers",
        "appsync:ListResolversByFunction",
        "appsync:ListTypes",
        "appsync:StartSchemaCreation",
        "appsync:UntagResource",
        "appsync:UpdateApiKey",
        "appsync:UpdateDataSource",
        "appsync:UpdateFunction",
        "appsync:UpdateResolver",
        "appsync:UpdateType",
        "appsync:TagResource",
        "appsync:CreateGraphqlApi",
        "appsync:DeleteGraphqlApi",
        "appsync:GetGraphqlApi",
        "appsync:ListTagsForResource",
        "appsync:UpdateGraphqlApi",
        "apigateway:DELETE",
        "apigateway:GET",
        "apigateway:PATCH",
        "apigateway:POST",
```

```
        "apigateway:PUT",
        "cognito-idp:CreateUserPool",
        "cognito-identity:CreateIdentityPool",
        "cognito-identity:DeleteIdentityPool",
        "cognito-identity:DescribeIdentity",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:SetIdentityPoolRoles",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:UpdateIdentityPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:CreateGroup",
        "cognito-idp:DeleteGroup",
        "cognito-identity:TagResource",
        "cognito-idp:TagResource",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:SetUserPoolMfaConfig",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeAsync",
        "lambda:InvokeFunction",
        "lambda:RemovePermission",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:AddLayerVersionPermission",
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping",
        "lambda:DeleteLayerVersion",
        "lambda:GetEventSourceMapping",
        "lambda:GetLayerVersion",
        "lambda:ListEventSourceMappings",
        "lambda:ListLayerVersions",
```

```
        "lambda:PublishLayerVersion",
        "lambda:RemoveLayerVersionPermission",
        "lambda:UpdateEventSourceMapping",
        "dynamodb:CreateTable",
        "dynamodb:DeleteItem",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListStreams",
        "dynamodb:PutItem",
        "dynamodb:TagResource",
        "dynamodb:ListTagsOfResource",
        "dynamodb:UntagResource",
        "dynamodb:UpdateContinuousBackups",
        "dynamodb:UpdateItem",
        "dynamodb:UpdateTable",
        "dynamodb:UpdateTimeToLive",
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketWebsite",
        "s3:PutObjectAcl",
        "cloudfront:CreateCloudFrontOriginAccessIdentity",
        "cloudfront:CreateDistribution",
        "cloudfront:DeleteCloudFrontOriginAccessIdentity",
        "cloudfront:DeleteDistribution",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetCloudFrontOriginAccessIdentityConfig",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:TagResource",
        "cloudfront:UntagResource",
        "cloudfront:UpdateCloudFrontOriginAccessIdentity",
        "cloudfront:UpdateDistribution",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
```

```
        "mobiletargeting:GetApp",
        "kinesis:AddTagsToStream",
        "kinesis:CreateStream",
        "kinesis:DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListTagsForStream",
        "kinesis:PutRecords",
        "es:AddTags",
        "es:CreateElasticsearchDomain",
        "es:DeleteElasticsearchDomain",
        "es:DescribeElasticsearchDomain",
        "es:UpdateElasticsearchDomainConfig",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CLISDKCalls",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetIntrospectionSchema",
        "appsync:GraphQL",
        "appsync:UpdateApiKey",
        "appsync:ListApiKeys",
        "amplify:*",
        "amplifybackend:*",
        "amplifyuibuilder:*",
        "sts:AssumeRole",
        "mobiletargeting:*",
        "cognito-idp:AdminAddUserToGroup",
        "cognito-idp:AdminCreateUser",
        "cognito-idp:CreateGroup",
        "cognito-idp:DeleteGroup",
        "cognito-idp:DeleteUser",
        "cognito-idp:ListUsers",
```

```
        "cognito-idp:AdminGetUser",
        "cognito-idp:ListUsersInGroup",
        "cognito-idp:AdminDisableUser",
        "cognito-idp:AdminRemoveUserFromGroup",
        "cognito-idp:AdminResetUserPassword",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:ListGroups",
        "cognito-idp:AdminListUserAuthEvents",
        "cognito-idp:AdminDeleteUser",
        "cognito-idp:AdminConfirmSignUp",
        "cognito-idp:AdminEnableUser",
        "cognito-idp:AdminUpdateUserAttributes",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:CreateUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:AdminSetUserPassword",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:SetIdentityPoolRoles",
        "cognito-identity:CreateIdentityPool",
        "cognito-identity:DeleteIdentityPool",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:DescribeIdentityPool",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "lambda:GetFunction",
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "lambda:DeleteFunction",
        "lambda:DeleteLayerVersion",
        "lambda:InvokeFunction",
        "lambda:ListLayerVersions",
        "iam:PutRolePolicy",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
        "iam:ListPolicyVersions",
        "iam:ListAttachedRolePolicies",
```

```
        "iam:CreateRole",
        "iam:PassRole",
        "iam:ListRolePolicies",
        "iam:DeleteRolePolicy",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:DeleteRole",
        "iam:DetachRolePolicy",
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks",
        "sns:CreateSMSSandboxPhoneNumber",
        "sns:GetSMSSandboxAccountStatus",
        "sns:VerifySMSSandboxPhoneNumber",
        "sns:DeleteSMSSandboxPhoneNumber",
        "sns:ListSMSSandboxPhoneNumbers",
        "sns:ListOriginationNumbers",
        "rekognition:DescribeCollection",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "lex:GetBot",
        "lex:GetBuiltinIntent",
        "lex:GetBuiltinIntents",
        "lex:GetBuiltinSlotTypes",
        "cloudformation:GetTemplateSummary",
        "codecommit:GitPull",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetCloudFrontOriginAccessIdentityConfig",
        "polly:DescribeVoices"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifySSMCalls",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:GetParametersByPath",
        "ssm:GetParameters",
        "ssm:GetParameter",
        "ssm:DeleteParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*"
    },
```

```
    {
      "Sid" : "GeoPowerUser",
      "Effect" : "Allow",
      "Action" : [
        "geo:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifyEcrSDKCalls",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifyStorageSDKCalls",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteBucketWebsite",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutBucketWebsite",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AmplifySSRCalls",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:CreateCloudFrontOriginAccessIdentity",
        "cloudfront:CreateDistribution",
        "cloudfront:CreateInvalidation",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByLambdaFunction",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListFieldLevelEncryptionConfigs",
        "cloudfront:ListFieldLevelEncryptionProfiles",
        "cloudfront:ListInvalidations",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListStreamingDistributions",
        "cloudfront:UpdateDistribution",
        "cloudfront:TagResource",
        "cloudfront:UntagResource",
        "cloudfront:ListTagsForResource",
        "cloudfront:DeleteDistribution",
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole",
        "iam:PutRolePolicy",
        "iam:PassRole",
        "lambda:CreateFunction",
        "lambda:EnableReplication",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "route53:ChangeResourceRecordSets",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "s3:CreateBucket",
```

```
        "s3:GetAccelerateConfiguration",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutObject",
        "s3:PutBucketTagging",
        "s3:GetBucketTagging",
        "lambda:ListEventSourceMappings",
        "lambda:CreateEventSourceMapping",
        "iam:UpdateAssumeRolePolicy",
        "iam:DeleteRolePolicy",
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:SetQueueAttributes",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:UpdateApp",
        "amplify:UpdateBranch"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifySSRViewLogGroups",
      "Effect" : "Allow",
      "Action" : "logs:DescribeLogGroups",
      "Resource" : "arn:aws:logs:*:*:log-group:*"
    },
    {
      "Sid" : "AmplifySSRCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/amplify/*"
    },
    {
      "Sid" : "AmplifySSRPushLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/amplify/*:log-stream:*"
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AdministratorAccess-AWSElasticBeanstalk

Descrição: concede permissões administrativas à conta. Permite explicitamente que desenvolvedores e administradores obtenham acesso direto aos recursos necessários para gerenciar aplicativos do AWS Elastic Beanstalk

`AdministratorAccess-AWSElasticBeanstalk` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AdministratorAccess-AWSElasticBeanstalk` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 22 de janeiro de 2021, 19:36 UTC
- Horário editado: 19 de maio de 2026, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:Describe*",
        "acm:List*",
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:Validate*",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "codecommit:Get*",
        "codecommit:UploadArchive",
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroup*",
        "ec2:CreateLaunchTemplate*",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteLaunchTemplate*",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroup*",
        "ecs:CreateCluster",
        "ecs:DeRegisterTaskDefinition",
        "ecs:Describe*",
        "ecs:List*",
        "ecs:RegisterTaskDefinition",
        "elasticbeanstalk:*",
        "elasticloadbalancing:Describe*",
        "iam:GetRole",
```

```
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "logs:Describe*",
        "rds:Describe*",
        "s3:ListAllMyBuckets",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:*"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CancelUpdateStack",
        "cloudformation:ContinueUpdateRollback",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:SignalResource",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:awseb-*",
        "arn:aws:cloudwatch:*:*:alarm:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:StartBuild"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/Elastic-Beanstalk-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable",
        "dynamodb:TagResource"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/awseb-e-*",
        "arn:aws:dynamodb:*:*:table/eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
```

```
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteCluster"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:*Rule",
        "elasticloadbalancing:*Tags",
        "elasticloadbalancing:SetRulePriorities",
        "elasticloadbalancing:SetSecurityGroups"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:*"
      ],
```

```
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/eb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/*/awseb-*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/*/eb-*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/eb-*/*/*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-elasticbeanstalk*",
        "arn:aws:iam::*:instance-profile/aws-elasticbeanstalk*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk*",
      "Condition" : {
        "ArnLike" : {
          "iam:PolicyArn" : [
            "arn:aws:iam::aws:policy/AWSElasticBeanstalk*",
            "arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalk*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/autoscaling.amazonaws.com/
AWSServiceRoleForAutoScaling",
        "arn:aws:iam::*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk",
        "arn:aws:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing",
        "arn:aws:iam::*:role/aws-service-role/
managedupdates.elasticbeanstalk.amazonaws.com/AWSServiceRoleForElasticBeanstalk",
        "arn:aws:iam::*:role/aws-service-role/
maintenance.elasticbeanstalk.amazonaws.com/AWSServiceRoleForElasticBeanstalk"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "elasticbeanstalk.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "managedupdates.elasticbeanstalk.amazonaws.com",
            "maintenance.elasticbeanstalk.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:*DBSubnetGroup",
        "rds:AuthorizeDBSecurityGroupIngress",
        "rds:CreateDBInstance",
        "rds:CreateDBSecurityGroup",
        "rds:DeleteDBInstance",
        "rds:DeleteDBSecurityGroup",
        "rds:ModifyDBInstance",
        "rds:RestoreDBInstanceFromDBSnapshot"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:secgrp:awseb-e-*",
        "arn:aws:rds:*:*:secgrp:eb-*",
        "arn:aws:rds:*:*:snapshot:*",
        "arn:aws:rds:*:*:subgrp:awseb-e-*",
        "arn:aws:rds:*:*:subgrp:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Delete*",
        "s3:Get*",
        "s3:Put*"
```

```
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucket*",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketOwnershipControls"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:GetTopicAttributes",
        "sns:Publish",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:*QueueAttributes",
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:SendMessage",
        "sqs:TagQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:awseb-e-*",
        "arn:aws:sqs:*:*:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AgentRegistryFullAccess

Descrição: Fornece acesso total ao AWS Agent Registry

`AgentRegistryFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AgentRegistryFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 06 de agosto de 2026, 18:12 UTC
- Horário editado: 31 de agosto de 2026, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AgentRegistryFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AgentRegistryFullAccess",
      "Effect" : "Allow",
      "Action" : "agent-registry:*",
      "Resource" : "arn:aws:agent-registry:*:*:*"
    },
    {
      "Sid" : "AgentRegistryPassRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "agent-registry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AgentRegistryWorkloadIdentityAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:CreateWorkloadIdentity",
        "bedrock-agentcore:DeleteWorkloadIdentity",
        "bedrock-agentcore:GetWorkloadAccessToken",
        "bedrock-agentcore:GetWorkloadIdentity"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:workload-identity-directory/*"
    },
    {
      "Sid" : "AllowGetResourceOauth2TokenForOauthBasedSynchronization",
```

```
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GetResourceOauth2Token"
      ],
      "Resource" : [
        "arn:aws:bedrock-agentcore:*:*:credential-provider/*",
        "arn:aws:bedrock-agentcore:*:*:workload-identity-directory/*",
        "arn:aws:bedrock-agentcore:*:*:token-vault/*/oauth2credentialprovider/*"
      ]
    },
    {
      "Sid" : "AllowListOauth2CredentialsProvidersForConsolePicker",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:ListOauth2CredentialProviders"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:*"
    },
    {
      "Sid" : "IAMListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "AgentRegistryKMSDecryptKeyForSynchronization",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AgentRegistryKMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
```

```
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "agent-registry.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AgentRegistryKMSCryptoOps",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "agent-registry.*.amazonaws.com",
          "kms:EncryptionContext:aws:agent-registry:registry-arn" : "arn:aws:agent-
registry:*:*:registry/*"
        }
      }
    },
    {
      "Sid" : "AgentRegistryKMSCreateGrant",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "agent-registry.*.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
```

```
            "ReEncryptTo",
            "DescribeKey",
            "CreateGrant"
          ]
        },
        "Null" : {
          "kms:GrantOperations" : "false"
        }
      }
    },
    {
      "Sid" : "AgentRegistrySecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*"
    },
    {
      "Sid" : "AgentRegistryServiceLinkedRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/agent-registry.amazonaws.com/
AWSServiceRoleForAgentRegistry",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "agent-registry.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AgentRegistryReadOnlyAccess

Descrição: Política de ReadOnly acesso ao AWS Agent Registry

`AgentRegistryReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AgentRegistryReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 06 de agosto de 2026, 18:12 UTC
- Horário editado: 06 de agosto de 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/AgentRegistryReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AgentRegistryReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "agent-registry:GetRegistry",
        "agent-registry:ListRegistries",
        "agent-registry:GetRegistryRecord",
        "agent-registry:ListRegistryRecords",
        "agent-registry:ListDiscoverableRegistryRecords",
        "agent-registry:GetDiscoverableRegistryRecord",
```

```
        "agent-registry:InvokeRegistryMcp",
        "agent-registry:SearchDiscoverableRegistryRecords",
        "agent-registry:ListTagsForResource"
      ],
      "Resource" : "arn:aws:agent-registry:*:*:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AIDevOpsAgentAccessPolicy

Descrição: Fornece as permissões exigidas pelo AWS DevOps agente para conduzir investigações e realizar análises sobre AWS os recursos do cliente.

`AIDevOpsAgentAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AIDevOpsAgentAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 26 de março de 2026, 03:42 UTC
- Horário editado: 24 de setembro de 2026, 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsAgentAccessPolicy`

Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOPSServiceWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:StartQuery",
        "support:CreateCase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AIOPSServiceAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:List*",
        "acm-pca:Describe*",
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:List*",
        "acm:DescribeCertificate",
        "acm:GetAccountConfiguration",
        "acm:GetCertificate",
        "acm:ListCertificates",
        "aidevops:GetAsset",
        "aidevops:GetAssetContent",
        "aidevops:GetAssetFile",
        "aidevops:GetKnowledgeItem",
        "aidevops:ListAssetFiles",
        "aidevops:ListAssets",
        "aidevops:ListAssetTypes",
        "aidevops:ListAssetVersions",
        "aidevops:ListKnowledgeItems",
        "airflow:GetEnvironment",
```

```
        "airflow:List*",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:List*",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:List*",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetEnvironment",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:List*",
        "appflow:Describe*",
        "appflow:List*",
        "application-autoscaling:Describe*",
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:List*",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "apprunner:Describe*",
        "apprunner:List*",
        "appstream:Describe*",
        "appstream:List*",
        "appsync:GetApiAssociation",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetFunction",
        "appsync:GetGraphqlApi",
        "appsync:GetGraphqlApiEnvironmentVariables",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResolver",
        "appsync:GetSourceApiAssociation",
        "appsync:List*",
        "aps:Describe*",
        "aps:List*",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:List*",
```

```
        "athena:GetCapacityAssignmentConfiguration",
        "athena:GetCapacityReservation",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAssessment",
        "auditmanager:List*",
        "autoscaling:Describe*",
        "backup-gateway:GetHypervisor",
        "backup-gateway:List*",
        "backup:Describe*",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:List*",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:List*",
        "bcm-data-exports:Get*",
        "bcm-data-exports:List*",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetCustomModel",
        "bedrock:GetDataSource",
        "bedrock:GetFoundationModel",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:List*",
        "budgets:Describe*",
        "budgets:List*",
        "budgets:ViewBudget",
        "ce:Describe*",
        "ce:Get*",
```

```
        "ce:List*",
        "chatbot:Describe*",
        "chatbot:GetMicrosoftTeamsChannelConfiguration",
        "chatbot:List*",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:List*",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:List*",
        "cloudformation:Describe*",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:List*",
        "cloudfront:Describe*",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetFunction",
        "cloudfront:GetKeyGroup",
        "cloudfront:GetMonitoringSubscription",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:List*",
        "cloudtrail:Describe*",
        "cloudtrail:GetChannel",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetQueryResults",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:List*",
```

```
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetInsightRuleReport",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricStream",
        "cloudwatch:GetOTelEnrichment",
        "cloudwatch:GetService",
        "cloudwatch:GetServiceLevelObjective",
        "cloudwatch:List*",
        "codeartifact:Describe*",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:List*",
        "codebuild:BatchGetFleets",
        "codebuild:List*",
        "codecommit:BatchDescribe*",
        "codecommit:BatchGet*",
        "codecommit:Describe*",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:GetApprovalRuleTemplate",
        "codecommit:GetBranch",
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
```

```
        "codecommit:List*",
        "codedeploy:BatchGetDeployments",
        "codedeploy:BatchGetDeploymentTargets",
        "codedeploy:GetApplication",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:GetDeploymentTarget",
        "codedeploy:List*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:List*",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:List*",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:List*",
        "codestar-notifications:Describe*",
        "codestar-notifications:List*",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeRiskConfiguration",
        "cognito-idp:DescribeUserImportJob",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:GetWebACLForResource",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListTagsForResource",
```

```
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:GetAggregateResourceConfig",
        "config:GetStoredQuery",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "connect:Describe*",
        "connect:GetMetricDataV2",
        "connect:GetTaskTemplate",
        "connect:List*",
        "cur:Describe*",
        "cur:Get*",
        "databrew:Describe*",
        "databrew:List*",
        "datapipeline:Describe*",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:List*",
        "datasync:Describe*",
        "datasync:List*",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetStorageProfile",
        "deadline:List*",
        "detective:GetMembers",
        "detective:List*",
        "devicefarm:GetDevicePool",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:GetVPCEConfiguration",
        "devicefarm:List*",
        "devops-guru:Describe*",
        "devops-guru:GetResourceCollection",
        "devops-guru:List*",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
```

```
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeHostedConnections",
        "directconnect:DescribeInterconnects",
        "directconnect:DescribeLags",
        "directconnect:DescribeTags",
        "directconnect:DescribeVirtualInterfaces",
        "dms:Describe*",
        "dms:List*",
        "ds:Describe*",
        "dynamodb:Describe*",
        "dynamodb:GetResourcePolicy",
        "dynamodb:List*",
        "ec2:Describe*",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetCapacityManagerAttributes",
        "ec2:GetCapacityManagerMetricData",
        "ec2:GetCapacityManagerMonitoredTagKeys",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ecr:Describe*",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:AccessKubernetesApi",
        "eks:Describe*",
        "eks:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
```

```
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:GetResourcePolicy",
        "elasticloadbalancing:GetTrustStoreCaCertificatesBundle",
        "elasticloadbalancing:GetTrustStoreRevocationContent",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "emr-containers:Describe*",
        "emr-containers:List*",
        "emr-serverless:GetApplication",
        "emr-serverless:List*",
        "es:Describe*",
        "es:List*",
        "events:Describe*",
        "events:List*",
        "evidently:GetExperiment",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:List*",
        "firehose:Describe*",
        "firehose:List*",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:List*",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:List*",
        "forecast:Describe*",
        "forecast:List*",
        "frauddetector:BatchGetVariable",
        "frauddetector:Describe*",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
```

```
        "frauddetector:GetVariables",
        "frauddetector:List*",
        "fsx:Describe*",
        "gamelift:Describe*",
        "gamelift:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:BatchGetJobs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlerMetrics",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDataQualityResult",
        "glue:GetJob",
        "glue:GetJobBookmark",
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:getPartition",
        "glue:GetPartitions",
        "glue:GetRegistry",
        "glue:GetResourcePolicy",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetWorkflow",
        "glue:GetWorkflowRun",
        "glue:List*",
        "glue:querySchemaVersionMetadata",
        "grafana:Describe*",
        "grafana:List*",
        "greengrass:Describe*",
        "greengrass:GetDeployment",
        "greengrass:List*",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
```

```
        "groundstation:GetMissionProfile",
        "groundstation:List*",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:List*",
        "health:Describe*",
        "healthlake:Describe*",
        "healthlake:List*",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccountAliases",
        "iam:ListAttachedRolePolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListOpenIDConnectProviders",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
```

```
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:List*",
        "inspector2:List*",
        "inspector2:SearchVulnerabilities",
        "inspector:Describe*",
        "inspector:List*",
        "internetmonitor:GetMonitor",
        "internetmonitor:List*",
        "iot:Describe*",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetThingShadow",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:GetV2LoggingOptions",
        "iot:List*",
        "iotanalytics:Describe*",
        "iotanalytics:List*",
        "iotevents:Describe*",
        "iotevents:List*",
        "iotsitewise:Describe*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:List*",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:List*",
```

```
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:List*",
        "kafka:Describe*",
        "kafka:GetClusterPolicy",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:Describe*",
        "kendra:List*",
        "kinesis:Describe*",
        "kinesis:GetResourcePolicy",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kms:DescribeCustomKeyStores",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:GetParametersForImport",
        "kms:GetPublicKey",
        "kms:ListAliases",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeyRotations",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "kms:ListRetirableGrants",
        "lakeformation:Describe*",
        "lakeformation:GetLFTag",
        "lakeformation:GetResourceLFTags",
        "lakeformation:List*",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
```

```
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
        "launchwizard:GetDeployment",
        "launchwizard:List*",
        "license-manager:GetLicense",
        "license-manager:List*",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:List*",
        "macie2:GetAllowList",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetMacieSession",
```

```
        "macie2:List*",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:Describe*",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:List*",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:List*",
        "memorydb:Describe*",
        "memorydb:List*",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:List*",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:Describe*",
        "network-firewall:List*",
        "networkmanager:Describe*",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:List*",
```

```
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:List*",
        "omics:GetAnnotationStore",
        "omics:GetReferenceStore",
        "omics:GetRunGroup",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:List*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:List*",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:List*",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:List*",
        "personalize:Describe*",
        "personalize:List*",
        "pi:Describe*",
        "pi:Get*",
        "pi:List*",
        "pipes:Describe*",
        "pipes:List*",
        "proton:GetEnvironmentTemplate",
        "proton:GetServiceTemplate",
        "proton:List*",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:List*",
```

```
        "ram:GetPermission",
        "ram:GetResourceShares",
        "ram:List*",
        "rds:Describe*",
        "rds:List*",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:List*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resiliencehub:Describe*",
        "resiliencehub:Get*",
        "resiliencehub:List*",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:List*",
        "resource-explorer-2:Search",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:List*",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:List*",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHealthCheckStatus",
        "route53:GetHostedZone",
        "route53:List*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:List*",
```

```
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:List*",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListOutpostsWithS3",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
```

```
            "s3:GetMultiRegionAccessPoint",
            "s3:GetMultiRegionAccessPointPolicy",
            "s3:GetMultiRegionAccessPointPolicyStatus",
            "s3:GetReplicationConfiguration",
            "s3:GetStorageLensConfiguration",
            "s3:GetStorageLensConfigurationTagging",
            "s3:GetStorageLensGroup",
            "s3:ListAllMyBuckets",
            "s3:ListTagsForResource",
            "sagemaker:Describe*",
            "sagemaker:List*",
            "scheduler:GetSchedule",
            "scheduler:GetScheduleGroup",
            "scheduler:List*",
            "schemas:Describe*",
            "schemas:GetResourcePolicy",
            "schemas:List*",
            "secretsmanager:Describe*",
            "secretsmanager:GetResourcePolicy",
            "secretsmanager:List*",
            "securityhub:BatchGetAutomationRules",
            "securityhub:BatchGetSecurityControls",
            "securityhub:Describe*",
            "securityhub:GetConfigurationPolicy",
            "securityhub:GetConfigurationPolicyAssociation",
            "securityhub:GetEnabledStandards",
            "securityhub:GetFindingAggregator",
            "securityhub:GetFindings",
            "securityhub:GetInsights",
            "securityhub:List*",
            "securitylake:GetSubscriber",
            "securitylake:List*",
            "servicecatalog:Describe*",
            "servicecatalog:GetApplication",
            "servicecatalog:GetAttributeGroup",
            "servicecatalog:List*",
            "servicequotas:Get*",
            "servicequotas:List*",
            "ses:Describe*",
            "ses:GetAccount",
            "ses:GetAddonInstance",
            "ses:GetAddonSubscription",
            "ses:GetArchive",
            "ses:GetConfigurationSet",
```

```
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailIdentity",
        "ses:GetEmailTemplate",
        "ses:GetIngressPoint",
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:List*",
        "shield:Describe*",
        "shield:List*",
        "signer:GetSigningProfile",
        "signer:List*",
        "sns:GetDataProtectionPolicy",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:List*",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:List*",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:List*",
        "ssm-sap:GetApplication",
        "ssm-sap:List*",
        "ssm:Describe*",
        "ssm:GetCommandInvocation",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetParameters",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:List*",
        "sso:DescribeAccountAssignmentCreationStatus",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetManagedApplicationInstance",
        "sso:GetPermissionsBoundaryForPermissionSet",
```

```
        "sso:GetSharedSsoConfiguration",
        "sso:ListAccountAssignments",
        "sso:ListApplicationAssignments",
        "sso:ListApplications",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:GetExecutionHistory",
        "states:Describe*",
        "states:List*",
        "support:DescribeCases",
        "synthetics:Describe*",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:List*",
        "tag:GetResources",
        "timestream:Describe*",
        "timestream:List*",
        "transfer:Describe*",
        "transfer:List*",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:List*",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:List*",
        "wafv2:GetIPSet",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRegexPatternSet",
        "wafv2:GetRuleGroup",
```

```
        "wafv2:GetSampledRequests",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:List*",
        "wisdom:Get*",
        "wisdom:List*",
        "wisdom:Query*",
        "wisdom:Retrieve",
        "wisdom:Search*",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:List*",
        "workspaces:Describe*",
        "xray:BatchGetTraces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetServiceGraph",
        "xray:GetTraceSummaries",
        "xray:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AIOPSAPIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
```

```
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*"
      ]
    },
    {
      "Sid" : "AllowListBucketAWSLogs",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "AWSLogs/*",
            "*/AWSLogs/*"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AIDevOpsAgentActionsPolicy

Descrição: Fornece permissões elevadas exigidas pelo AWS DevOps agente para realizar mutações aprovadas pelo operador ou ações elevadas nos AWS recursos do cliente durante eventos operacionais.

`AIDevOpsAgentActionsPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AIDevOpsAgentActionsPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 23 de junho de 2026, 22:27 UTC
- Horário editado: 19 de agosto de 2026, 22:47 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsAgentActionsPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIDevOpsElevatedAccess",
      "Effect" : "Allow",
      "NotAction" : [
        "account:*",
        "cognito-identity:*",
        "iam:*",
```

```
        "identitystore:*",
        "organizations:*",
        "ram:*",
        "rolesanywhere:*",
        "sso:*",
        "sts:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AIDevOpsElevatedCarveBacks",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetGovCloudAccountInformation",
        "account:GetPrimaryEmail",
        "account:ListRegions",
        "iam:ListRoles",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "sts:DecodeAuthorizationMessage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AIDevOpsAgentFullAccess

Descrição: Fornece acesso total ao Amazon DevOps Agent por meio do Console de gerenciamento da AWS

`AIDevOpsAgentFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AIDevOpsAgentFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 26 de março de 2026, 03:42 UTC
- Horário editado: 26 de junho de 2026, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsAgentFullAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIDevOpsAgentAccess",
      "Effect" : "Allow",
      "Action" : [
        "aidevops:AllowVendedLogDeliveryForResource",
        "aidevops:AssociateService",
        "aidevops:CreateAccessToken",
        "aidevops:CreateAgentSpace",
        "aidevops:CreateAsset",
        "aidevops:CreateAssetFile",
        "aidevops:CreateBacklogTask",
        "aidevops:CreateChat",
        "aidevops:CreateKnowledgeItem",
        "aidevops:CreateOneTimeLoginSession",
        "aidevops:CreatePrivateConnection",
        "aidevops:CreateTrigger",
```

```
        "aidevops:DeleteAgentSpace",
        "aidevops:DeleteAsset",
        "aidevops:DeleteAssetFile",
        "aidevops:DeleteKnowledgeItem",
        "aidevops:DeletePrivateConnection",
        "aidevops:DeleteTrigger",
        "aidevops:DeregisterService",
        "aidevops:DescribePrivateConnection",
        "aidevops:DescribeServices",
        "aidevops:DescribeSupportLevel",
        "aidevops:DisableOperatorApp",
        "aidevops:DisassociateService",
        "aidevops:DiscoverTopology",
        "aidevops:EnableOperatorApp",
        "aidevops:EndChatForCase",
        "aidevops:GetAccessToken",
        "aidevops:GetAccountUsage",
        "aidevops:GetAgentSpace",
        "aidevops:GetAsset",
        "aidevops:GetAssetContent",
        "aidevops:GetAssetFile",
        "aidevops:GetAssociation",
        "aidevops:GetBacklogTask",
        "aidevops:GetKnowledgeItem",
        "aidevops:GetOperatorApp",
        "aidevops:GetRecommendation",
        "aidevops:GetService",
        "aidevops:GetTrigger",
        "aidevops:InitiateChatForCase",
        "aidevops:ListAccessTokens",
        "aidevops:ListAgentSpaces",
        "aidevops:ListAssetFiles",
        "aidevops:ListAssets",
        "aidevops:ListAssetTypes",
        "aidevops:ListAssetVersions",
        "aidevops:ListAssociations",
        "aidevops:ListBacklogTasks",
        "aidevops:ListChats",
        "aidevops:ListExecutions",
        "aidevops:ListGoals",
        "aidevops:ListJournalRecords",
        "aidevops:ListKnowledgeItems",
        "aidevops:ListKnowledgeItemVersions",
        "aidevops:ListPendingMessages",
```

```
        "aidevops:ListPrivateConnections",
        "aidevops:ListRecommendations",
        "aidevops:ListServices",
        "aidevops:ListTagsForResource",
        "aidevops:ListTriggers",
        "aidevops:ListWebhooks",
        "aidevops:RegisterService",
        "aidevops:RevokeAccessToken",
        "aidevops:RotateAccessToken",
        "aidevops:SearchServiceAccessibleResource",
        "aidevops:SendMessage",
        "aidevops:TagResource",
        "aidevops:UntagResource",
        "aidevops:UpdateAgentSpace",
        "aidevops:UpdateApprovalAction",
        "aidevops:UpdateAsset",
        "aidevops:UpdateAssetFile",
        "aidevops:UpdateAssociation",
        "aidevops:UpdateBacklogTask",
        "aidevops:UpdateGoal",
        "aidevops:UpdateKnowledgeItem",
        "aidevops:UpdateOperatorAppIdpConfig",
        "aidevops:UpdatePrivateConnectionCertificate",
        "aidevops:UpdateRecommendation",
        "aidevops:UpdateTrigger",
        "aidevops:ValidateAwsAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AIDevOpsAgentReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon DevOps Agent por meio do Console de gerenciamento da AWS

`AIDevOpsAgentReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AIDevOpsAgentReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 26 de março de 2026, 03:42 UTC
- Horário editado: 11 de junho de 2026, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsAgentReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIDevOpsAgentReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aidevops:DescribePrivateConnection",
        "aidevops:DescribeServices",
        "aidevops:Get*",
```

```
        "aidevops:List*",
        "aidevops:SearchServiceAccessibleResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AIDevOpsChannelAccessPolicy

Descrição: Forneça acesso ao bate-papo e gerencie investigações por meio do AWS DevOps Agente para seu AgentSpaces

`AIDevOpsChannelAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AIDevOpsChannelAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 26 de agosto de 2026, 21:07 UTC
- Horário editado: 26 de agosto de 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AIDevOpsChannelAccessPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowChatActions",
      "Effect" : "Allow",
      "Action" : [
        "aidevops:CreateChat",
        "aidevops:SendMessage"
      ],
      "Resource" : "arn:aws:aidevops:*:*:agentspace/${aws:PrincipalTag/AgentSpaceId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AIDevOpsConstellationAccessPolicy

Descrição: Fornece as permissões exigidas pelo AWS DevOps Agente para coordenar com os AgentSpaces conectados por meio da Constelação Espacial do Agente.

`AIDevOpsConstellationAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AIDevOpsConstellationAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 05 de agosto de 2026, 16:27 UTC
- Horário editado: 05 de agosto de 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AIDevOpsConstellationAccessPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConstellationCoordination",
      "Effect" : "Allow",
      "Action" : [
        "aidevops:GetAgentSpace",
        "aidevops:CreateBacklogTask",
        "aidevops:GetBacklogTask",
        "aidevops:ListBacklogTasks",
        "aidevops:GetAsset",
        "aidevops:GetAssetContent",
        "aidevops:GetAssetFile",
        "aidevops:ListAssets",
        "aidevops:ListAssetFiles",
```

```
        "aidevops:ListExecutions",
        "aidevops:ListJournalRecords"
      ],
      "Resource" : "arn:aws:aidevops:*:*:agentspace/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AIDevOpsOperatorAppAccessPolicy

Descrição: Fornece acesso para usar o aplicativo web do AWS DevOps operador para um Agent Space.

`AIDevOpsOperatorAppAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AIDevOpsOperatorAppAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 26 de março de 2026, 03:42 UTC
- Horário editado: 10 de setembro de 2026, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsOperatorAppAccessPolicy`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOperatorAgentSpaceActions",
      "Effect" : "Allow",
      "Action" : [
        "aidevops:CreateAccessToken",
        "aidevops:CreateAsset",
        "aidevops:CreateAssetFile",
        "aidevops:CreateBacklogTask",
        "aidevops:CreateChat",
        "aidevops:CreateKnowledgeItem",
        "aidevops:CreateTrigger",
        "aidevops:DeleteAsset",
        "aidevops:DeleteAssetFile",
        "aidevops:DeleteKnowledgeItem",
        "aidevops:DeleteTrigger",
        "aidevops:DescribeServices",
        "aidevops:DescribeSupportLevel",
        "aidevops:DiscoverTopology",
        "aidevops:EndChatForCase",
        "aidevops:GetAccessToken",
        "aidevops:GetAgentSpace",
        "aidevops:GetAsset",
        "aidevops:GetAssetContent",
        "aidevops:GetAssetFile",
        "aidevops:GetAssociation",
        "aidevops:GetBacklogTask",
        "aidevops:GetKnowledgeItem",
        "aidevops:GetRecommendation",
        "aidevops:GetTrigger",
        "aidevops:InitiateChatForCase",
        "aidevops:ListAccessTokens",
        "aidevops:ListAssetFiles",
        "aidevops:ListAssets",
        "aidevops:ListAssetTypes",
```

```
        "aidevops:ListAssetVersions",
        "aidevops:ListAssociations",
        "aidevops:ListBacklogTasks",
        "aidevops:ListChats",
        "aidevops:ListExecutions",
        "aidevops:ListGoals",
        "aidevops:ListJournalRecords",
        "aidevops:ListKnowledgeItems",
        "aidevops:ListKnowledgeItemVersions",
        "aidevops:ListPendingMessages",
        "aidevops:ListRecommendations",
        "aidevops:ListTriggers",
        "aidevops:ListWebhooks",
        "aidevops:RevokeAccessToken",
        "aidevops:RotateAccessToken",
        "aidevops:SendMessage",
        "aidevops:UpdateApprovalAction",
        "aidevops:UpdateAsset",
        "aidevops:UpdateAssetFile",
        "aidevops:UpdateBacklogTask",
        "aidevops:UpdateGoal",
        "aidevops:UpdateKnowledgeItem",
        "aidevops:UpdateRecommendation",
        "aidevops:UpdateTrigger"
      ],
      "Resource" : [
        "arn:aws:aidevops:*:*:agentspace/${aws:PrincipalTag/AgentSpaceId}",
        "arn:aws:aidevops:*:*:agentspace/${aws:PrincipalTag/AgentSpaceId}/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorAccountActions",
      "Effect" : "Allow",
      "Action" : [
        "aidevops:GetAccountUsage"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSupportOperatorActions",
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeCases",
        "support:DescribeServices",
        "support:InitiateChatForCase",
        "support:DescribeSupportLevel"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSecretsManagerOperatorActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowTranscribeOperatorActions",
      "Effect" : "Allow",
      "Action" : [
        "transcribe:StartStreamTranscriptionWebSocket"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AIDevOpsReleaseManagementVPCPolicy

Descrição: fornece permissões para que o AWS DevOps agente crie e gerencie interfaces de rede em sua VPC para que os agentes de gerenciamento de versões possam acessar recursos privados

`AIDevOpsReleaseManagementVPCPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AIDevOpsReleaseManagementVPCPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 21 de agosto de 2026, 22:27 UTC
- Horário editado: 21 de agosto de 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AIDevOpsReleaseManagementVPCPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ManagedByVerificationTesting" : [
            ""
          ],
```

```
          "ec2:CreateAction" : "CreateNetworkInterface",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedByVerificationTesting" : "",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "ManagedByVerificationTesting"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/ManagedByVerificationTesting" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AIOpsAssistantIncidentReportPolicy

Descrição: fornece as permissões exigidas pelo assistente do Amazon AI Operations para gerar um relatório de incidentes da investigação.

`AIOpsAssistantIncidentReportPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AIOpsAssistantIncidentReportPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Tempo de criação: 10 de outubro de 2025, 22:04 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsAssistantIncidentReportPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
```

```
      "Action" : [
        "aiops:PutFact",
        "aiops:UpdateReport",
        "aiops:GetReport",
        "aiops:GenerateReport",
        "aiops:CreateReport",
        "aiops:GetFact",
        "aiops:ListFacts",
        "aiops:GetFactVersions",
        "aiops:GetInvestigation",
        "aiops:ListInvestigationEvents",
        "aiops:GetInvestigationEvent"
      ],
      "Resource" : [
        "arn:aws:aiops:*:*:investigation-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AIOpsAssistantPolicy

Descrição: Fornece ReadOnly as permissões exigidas pelo Amazon AI Operations Assistant para fazer análises dos AWS recursos do cliente durante as investigações.

`AIOpsAssistantPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AIOpsAssistantPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 02 de dezembro de 2024, 16:21 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsAssistantPolicy`

Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOPSServiceAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:List*",
        "acm-pca:Describe*",
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:List*",
        "acm:DescribeCertificate",
        "acm:GetAccountConfiguration",
        "airflow:List*",
        "amplify:GetApp",
        "amplify:GetBranch",
```

```
        "amplify:GetDomainAssociation",
        "amplify:List*",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:List*",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetEnvironment",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:List*",
        "appflow:Describe*",
        "appflow:List*",
        "application-autoscaling:Describe*",
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:List*",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "apprunner:Describe*",
        "apprunner:List*",
        "appstream:Describe*",
        "appstream:List*",
        "appsync:GetApiAssociation",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetFunction",
        "appsync:GetGraphqlApi",
        "appsync:GetGraphqlApiEnvironmentVariables",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResolver",
        "appsync:GetSourceApiAssociation",
        "appsync:List*",
        "aps:Describe*",
        "aps:List*",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:List*",
        "athena:GetCapacityAssignmentConfiguration",
        "athena:GetCapacityReservation",
        "athena:GetDataCatalog",
```

```
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAssessment",
        "auditmanager:List*",
        "autoscaling:Describe*",
        "backup-gateway:GetHypervisor",
        "backup-gateway:List*",
        "backup:Describe*",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:List*",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:List*",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetDataSource",
        "bedrock:GetGuardrail",
        "bedrock:GetKnowledgeBase",
        "bedrock:List*",
        "budgets:Describe*",
        "budgets:List*",
        "ce:Describe*",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:List*",
        "chatbot:Describe*",
        "chatbot:GetMicrosoftTeamsChannelConfiguration",
        "chatbot:List*",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:List*",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
```

```
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:List*",
        "cloudformation:Describe*",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:List*",
        "cloudfront:Describe*",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetFunction",
        "cloudfront:GetKeyGroup",
        "cloudfront:GetMonitoringSubscription",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:List*",
        "cloudtrail:Describe*",
        "cloudtrail:GetChannel",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetQueryResults",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartQuery",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetInsightRuleReport",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricStream",
        "cloudwatch:GetService",
```

```
        "cloudwatch:GetServiceLevelObjective",
        "cloudwatch:List*",
        "codeartifact:Describe*",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:List*",
        "codebuild:BatchGetFleets",
        "codebuild:List*",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codedeploy:BatchGetDeployments",
        "codedeploy:BatchGetDeploymentTargets",
        "codedeploy:GetApplication",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:List*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:List*",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:List*",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:List*",
        "codestar-notifications:Describe*",
        "codestar-notifications:List*",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeRiskConfiguration",
        "cognito-idp:DescribeUserImportJob",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
```

```
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:GetWebACLForResource",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListTagsForResource",
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:GetStoredQuery",
        "config:List*",
        "connect:Describe*",
        "connect:GetTaskTemplate",
        "connect:List*",
        "databrew:Describe*",
        "databrew:List*",
        "datapipeline:Describe*",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:List*",
        "datasync:Describe*",
        "datasync:List*",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetStorageProfile",
        "deadline:List*",
        "detective:GetMembers",
        "detective:List*",
        "devicefarm:GetDevicePool",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:GetVPCEConfiguration",
        "devicefarm:List*",
        "devops-guru:Describe*",
        "devops-guru:GetResourceCollection",
```

```
        "devops-guru:List*",
        "dms:Describe*",
        "dms:List*",
        "ds:Describe*",
        "dynamodb:Describe*",
        "dynamodb:GetResourcePolicy",
        "dynamodb:List*",
        "ec2:Describe*",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ecr:Describe*",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
        "eks:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:GetResourcePolicy",
        "elasticloadbalancing:GetTrustStoreCaCertificatesBundle",
        "elasticloadbalancing:GetTrustStoreRevocationContent",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "emr-containers:Describe*",
        "emr-containers:List*",
```

```
        "emr-serverless:GetApplication",
        "emr-serverless:List*",
        "es:Describe*",
        "es:List*",
        "events:Describe*",
        "events:List*",
        "evidently:GetExperiment",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:List*",
        "firehose:Describe*",
        "firehose:List*",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:List*",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:List*",
        "forecast:Describe*",
        "forecast:List*",
        "frauddetector:BatchGetVariable",
        "frauddetector:Describe*",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:List*",
        "fsx:Describe*",
        "gamelift:Describe*",
        "gamelift:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:GetDatabase",
        "glue:GetDatabases",
```

```
        "glue:GetJob",
        "glue:GetRegistry",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:List*",
        "glue:querySchemaVersionMetadata",
        "grafana:Describe*",
        "grafana:List*",
        "greengrass:Describe*",
        "greengrass:GetDeployment",
        "greengrass:List*",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:List*",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:List*",
        "health:DescribeEvents",
        "health:DescribeEventDetails",
        "healthlake:Describe*",
        "healthlake:List*",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetUser",
        "iam:GetUserPolicy",
```

```
        "iam:ListAttachedRolePolicies",
        "iam:ListOpenIDConnectProviders",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:List*",
        "inspector2:List*",
        "inspector:Describe*",
        "inspector:List*",
        "internetmonitor:GetMonitor",
        "internetmonitor:List*",
        "iot:Describe*",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetThingShadow",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:GetV2LoggingOptions",
        "iot:List*",
        "iotanalytics:Describe*",
        "iotanalytics:List*",
        "iotevents:Describe*",
        "iotevents:List*",
        "iotfleethub:Describe*",
        "iotfleethub:List*",
        "iotsitewise:Describe*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
```

```
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:List*",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:List*",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:List*",
        "kafka:Describe*",
        "kafka:GetClusterPolicy",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:Describe*",
        "kendra:List*",
        "kinesis:Describe*",
        "kinesis:GetResourcePolicy",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kms:DescribeKey",
        "kms:ListResourceTags",
        "kms:ListKeys",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeyRotations",
        "lakeformation:Describe*",
        "lakeformation:GetLFTag",
        "lakeformation:GetResourceLFTags",
        "lakeformation:List*",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
```

```
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
        "launchwizard:GetDeployment",
        "launchwizard:List*",
        "lex:Describe*",
        "lex:List*",
        "license-manager:GetLicense",
        "license-manager:List*",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:List*",
        "logs:StartQuery",
```

```
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "lookoutmetrics:Describe*",
        "lookoutmetrics:List*",
        "lookoutvision:Describe*",
        "lookoutvision:List*",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:List*",
        "macie2:GetAllowList",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetMacieSession",
        "macie2:List*",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:Describe*",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:List*",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:List*",
        "memorydb:Describe*",
        "memorydb:List*",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:List*",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:Describe*",
        "network-firewall:List*",
        "networkmanager:Describe*",
        "networkmanager:GetConnectAttachment",
```

```
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:List*",
        "nimble:GetLaunchProfile",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:List*",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:List*",
        "omics:GetAnnotationStore",
        "omics:GetReferenceStore",
        "omics:GetRunGroup",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:List*",
        "opsworks-cm:Describe*",
        "opsworks-cm:List*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:List*",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
```

```
        "pca-connector-ad:List*",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:List*",
        "personalize:Describe*",
        "personalize:List*",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pipes:Describe*",
        "pipes:List*",
        "proton:GetEnvironmentTemplate",
        "proton:GetServiceTemplate",
        "proton:List*",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:List*",
        "qldb:Describe*",
        "qldb:List*",
        "ram:GetPermission",
        "ram:List*",
        "rds:Describe*",
        "rds:List*",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:List*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:List*",
```

```
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:List*",
        "robomaker:Describe*",
        "robomaker:List*",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:List*",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:List*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:List*",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:List*",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:List*",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
```

```
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "S3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:List*",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:List*",
        "schemas:Describe*",
        "schemas:GetResourcePolicy",
        "schemas:List*",
        "secretsmanager:Describe*",
```

```
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetSecurityControls",
        "securityhub:Describe*",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:GetInsights",
        "securityhub:List*",
        "securitylake:GetSubscriber",
        "securitylake:List*",
        "servicecatalog:Describe*",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:List*",
        "servicequotas:GetServiceQuota",
        "ses:Describe*",
        "ses:GetAccount",
        "ses:GetAddonInstance",
        "ses:GetAddonSubscription",
        "ses:GetArchive",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailIdentity",
        "ses:GetEmailTemplate",
        "ses:GetIngressPoint",
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:List*",
        "shield:Describe*",
        "shield:List*",
        "signer:GetSigningProfile",
        "signer:List*",
        "sns:GetDataProtectionPolicy",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:List*",
```

```
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:List*",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:List*",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:List*",
        "ssm-sap:GetApplication",
        "ssm-sap:List*",
        "ssm:Describe*",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetParameters",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:List*",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetManagedApplicationInstance",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:GetSharedSsoConfiguration",
        "sso:ListAccountAssignments",
        "sso:ListApplicationAssignments",
        "sso:ListApplications",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListTagsForResource",
        "states:GetExecutionHistory",
        "states:Describe*",
        "states:List*",
        "synthetics:Describe*",
        "synthetics:GetCanary",
        "synthetics:GetGroup",
        "synthetics:List*",
        "tag:GetResources",
        "timestream:Describe*",
        "timestream:List*",
        "transfer:Describe*",
        "transfer:List*",
        "verifiedpermissions:GetIdentitySource",
```

```
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:List*",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:List*",
        "wafv2:GetIPSet",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRegexPatternSet",
        "wafv2:GetRuleGroup",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:List*",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:List*",
        "workspaces:Describe*",
        "xray:BatchGetTraces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetServiceGraph",
        "xray:GetTraceSummaries",
        "xray:List*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AIOPSS3AccessForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::amplify",
        "arn:aws:s3:::cdk--assets--*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ViaAWSService" : [
            "amplify.amazonaws.com"
          ],
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "AIOPSAPIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/stages",
```

```
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/domainnames/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AIOpsConsoleAdminPolicy

Descrição: Concede acesso total ao serviço Amazon AI Operations e às permissões necessárias por meio AWS do console. Isso também inclui permissões para usar as sessões do console com reconhecimento de identidade.

`AIOpsConsoleAdminPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AIOpsConsoleAdminPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Tempo de criação: 02 de dezembro de 2024, 23:51 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsConsoleAdminPolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOpsAdmin",
      "Effect" : "Allow",
      "Action" : [
        "aiops:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOApplicationManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:PutApplicationAccessScope",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAuthenticationMethod",
        "sso:DeleteApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:ResourceTag/ManagedByAmazonAIOperations" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "SSOApplicationTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:TagResource"
      ],
      "Resource" : [
        "arn:aws:sso:::instance/*",
        "arn:aws:sso::aws:applicationProvider/aiops"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:RequestTag/ManagedByAmazonAIOperations" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ManagedByAmazonAIOperations"
          ]
        }
      }
    },
    {
      "Sid" : "SSOTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:TagResource"
      ],
      "Resource" : "arn:aws:sso::*:application/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:ResourceTag/ManagedByAmazonAIOperations" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ManagedByAmazonAIOperations"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "sso:ListApplications",
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:DescribeInstance",
        "sso:GetSSOStatus",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSTSContextSetting",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "IdentityPropagationAccess",
      "Effect" : "Allow",
      "Action" : [
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudtrailAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListTrails",
        "cloudtrail:DescribeTrails",
        "cloudtrail:ListEventDataStores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMIntegrationSecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:aws/ssm/3p/*"
    },
    {
      "Sid" : "SSMIntegrationAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting",
        "ssm:UpdateServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/integrations/*"
    },
    {
      "Sid" : "SSMIntegrationCreatePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy"
      ],
      "Resource" : "arn:aws:iam::*:policy/service-role/
AWSServiceRoleSSMIntegrationsPolicy*"
    },
    {
      "Sid" : "ChatbotConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeChimeWebhookConfigurations",
        "chatbot:DescribeSlackWorkspaces",
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chatbot:ListMicrosoftTeamsConfiguredTeams"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "IAMPassRoleToAIOps",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "aiops.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagBoundaryPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleToSSMIntegration",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.integrations.amazonaws.com"
        },
        "ArnEquals" : {
          "iam:AssociatedResourceArn" : "arn:aws:aiops:*:*:investigation-group/*"
        }
```

```
      }
    },
    {
      "Sid" : "SSMOpsItemAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:*:ssm:*:*:opsitem/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Integration" : "CloudWatch",
          "aws:ResourceTag/Integration" : "CloudWatch"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Integration"
          ]
        }
      }
    },
    {
      "Sid" : "CreateAIOpsCrossAccountAssistantPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy"
      ],
      "Resource" : "arn:aws:iam::*:policy/AIOpsCrossAccountAssistantPolicy*"
    },
    {
      "Sid" : "AmazonQAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AIOpsOperatorAccess

Descrição: concede acesso às APIs do Amazon AI Operations para a criação, atualização e exclusão de investigações, eventos de investigação e recursos de investigação. Também inclui ReadOnly acesso a todas as APIs de operações de IA e o uso de sessões com reconhecimento de identidade.

`AIOpsOperatorAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AIOpsOperatorAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Tempo de criação: 02 de dezembro de 2024, 23:51 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsOperatorAccess`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOpsOperatorAccess",
      "Effect" : "Allow",
      "Action" : [
        "aiops:CreateInvestigation",
        "aiops:CreateInvestigationEvent",
        "aiops:CreateInvestigationResource",
        "aiops:DeleteInvestigation",
        "aiops:Get*",
        "aiops:List*",
        "aiops:UpdateInvestigation",
        "aiops:UpdateInvestigationEvent",
        "aiops:ValidateInvestigationGroup",
        "aiops:PutFact",
        "aiops:UpdateReport",
        "aiops:GenerateReport",
        "aiops:CreateReport",
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "sso:DescribeInstance",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowSTSContextSetting",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "SSMSettingServiceIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/integrations/*"
    },
    {
      "Sid" : "SSMIntegrationTagAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Integration" : [
            "CloudWatch"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "Integration"
        }
      }
    },
    {
      "Sid" : "SSMOpsItemIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/Integration" : [
            "CloudWatch"
          ]
        }
      }
    },
    {
      "Sid" : "SSMTagOperation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Integration" : [
            "CloudWatch"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "Integration"
        }
      }
    },
    {
      "Sid" : "SSMOpsSummaryIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsSummary"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AIOpsReadOnlyAccess

Descrição: Concede ReadOnly permissões ao serviço Amazon AI Operations e aos recursos necessários.

`AIOpsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AIOpsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Tempo de criação: 02 de dezembro de 2024, 23:51 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsReadOnlyAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOpsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aiops:Get*",
        "aiops:List*",
        "aiops:ValidateInvestigationGroup"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "sso:DescribeInstance",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AlexaForBusinessDeviceSetup

Descrição: Forneça acesso à configuração do dispositivo aos AlexaForBusiness serviços

`AlexaForBusinessDeviceSetup` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AlexaForBusinessDeviceSetup` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de novembro de 2017, 16:47 UTC
- Hora da edição: 20 de maio de 2019, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:RegisterDevice",
        "a4b:CompleteRegistration",
        "a4b:SearchDevices",
        "a4b:SearchNetworkProfiles",
        "a4b:GetNetworkProfile",
        "a4b:PutDeviceSetupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "A4bDeviceSetupAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4BNetworkProfile*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AlexaForBusinessFullAccess

Descrição: Concede acesso total aos AlexaForBusiness recursos e acesso a recursos relacionados Serviços da AWS

`AlexaForBusinessFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AlexaForBusinessFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de novembro de 2017, 16:47 UTC
- Hora da edição: 01 de julho de 2020, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessFullAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:*",
        "kms:DescribeKey"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "*a4b.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*a4b.amazonaws.com/
AWSServiceRoleForAlexaForBusiness*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4B*"
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "A4B*"
        }
      }
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AlexaForBusinessGatewayExecution

Descrição: Forneça acesso de execução de gateway aos AlexaForBusiness serviços

`AlexaForBusinessGatewayExecution` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AlexaForBusinessGatewayExecution` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de novembro de 2017, 16:47 UTC
- Hora da edição: 30 de novembro de 2017, 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:Send*",
        "a4b:Get*"
      ],
      "Resource" : "arn:aws:a4b:*:*:gateway/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:dd-*",
        "arn:aws:sqs:*:*:sd-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:List*",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AlexaForBusinessLifesizeDelegatedAccessPolicy

Descrição: fornece acesso a dispositivos Lifesize AVS

`AlexaForBusinessLifesizeDelegatedAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AlexaForBusinessLifesizeDelegatedAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 04 de junho de 2020, 19:46 UTC
- Hora da edição: 12 de junho de 2020, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "a4b:DisassociateDeviceFromRoom",
        "a4b:DeleteDevice",
        "a4b:UpdateDevice",
        "a4b:GetDevice"
      ],
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A2IWO7UEGWV4TL"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:RegisterAVSDevice"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "a4b:amazonId" : [
            "A2IWO7UEGWV4TL"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:SearchDevices"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "a4b:filters_deviceType" : [
            "*A2IWO7UEGWV4TL"
          ]
        },
        "Null" : {
          "a4b:filters_deviceType" : "false"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:AssociateDeviceWithRoom"
      ],
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A2IWO7UEGWV4TL",
        "arn:aws:a4b:us-east-1:*:room/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:GetRoom",
        "a4b:GetAddressBook",
        "a4b:SearchRooms",
        "a4b:CreateContact",
        "a4b:CreateRoom",
        "a4b:UpdateContact",
        "a4b:ListConferenceProviders",
        "a4b:DeleteRoom",
        "a4b:CreateAddressBook",
        "a4b:DisassociateContactFromAddressBook",
        "a4b:CreateConferenceProvider",
        "a4b:PutConferencePreference",
        "a4b:DeleteAddressBook",
        "a4b:AssociateContactWithAddressBook",
        "a4b:DeleteContact",
        "a4b:SearchProfiles",
        "a4b:UpdateProfile",
        "a4b:GetContact"
      ],
      "Resource" : "*"
    },
    {
      "Action" : [
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AlexaForBusinessNetworkProfileServicePolicy

Descrição: esta política permite que o Alexa for Business execute tarefas automatizadas agendadas pelos seus perfis de rede.

`AlexaForBusinessNetworkProfileServicePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 13 de março de 2019, 0:53 UTC
- Hora da edição: 5 de abril de 2019, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "A4bPcaTagAccess",
      "Action" : [
        "acm-pca:GetCertificate",
        "acm-pca:IssueCertificate",
        "acm-pca:RevokeCertificate"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/a4b" : "enabled"
        }
      }
    },
    {
      "Sid" : "A4bNetworkProfileAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4BNetworkProfile*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AlexaForBusinessPolyDelegatedAccessPolicy

Descrição: fornece acesso a dispositivos Poly AVS

`AlexaForBusinessPolyDelegatedAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AlexaForBusinessPolyDelegatedAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 16 de outubro de 2019, 19:48 UTC
- Hora da edição: 16 de outubro de 2019, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "a4b:DisassociateDeviceFromRoom",
        "a4b:DeleteDevice",
        "a4b:UpdateDevice",
        "a4b:GetDevice"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A238TWV36W3S92",
        "arn:aws:a4b:us-east-1:*:device/*/*:A1FUZ1SC53VJXD"
      ]
    },
    {
      "Action" : [
```

```
        "a4b:RegisterAVSDevice"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "a4b:amazonId" : [
            "A238TWV36W3S92",
            "A1FUZ1SC53VJXD"
          ]
        }
      }
    },
    {
      "Action" : [
        "a4b:SearchDevices"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "a4b:AssociateDeviceWithRoom"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A238TWV36W3S92",
        "arn:aws:a4b:us-east-1:*:device/*/*:A1FUZ1SC53VJXD",
        "arn:aws:a4b:us-east-1:*:room/*"
      ]
    },
    {
      "Action" : [
        "a4b:GetRoom",
        "a4b:SearchRooms",
        "a4b:CreateRoom",
        "a4b:GetProfile",
        "a4b:SearchSkillGroups",
        "a4b:DisassociateSkillGroupFromRoom",
        "a4b:AssociateSkillGroupWithRoom",
```

```
        "a4b:GetSkillGroup",
        "a4b:SearchProfiles",
        "a4b:GetAddressBook",
        "a4b:UpdateRoom"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AlexaForBusinessReadOnlyAccess

Descrição: Forneça acesso somente para leitura aos AlexaForBusiness serviços

`AlexaForBusinessReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AlexaForBusinessReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de novembro de 2017, 16:47 UTC
- Hora da edição: 20 de novembro de 2019, 0:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:Get*",
        "a4b:List*",
        "a4b:Search*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonAPIGatewayAdministrator

Descrição: Fornece acesso total às APIs create/edit /delete no Amazon API Gateway por meio do. Console de gerenciamento da AWS

`AmazonAPIGatewayAdministrator` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonAPIGatewayAdministrator` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de julho de 2015, 17:34 UTC
- Hora da edição: 09 de julho de 2015, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:*"
      ],
      "Resource" : "arn:aws:apigateway:*::/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonAPIGatewayInvokeFullAccess

Descrição: fornece acesso total para invocar APIs no Amazon API Gateway.

`AmazonAPIGatewayInvokeFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonAPIGatewayInvokeFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de julho de 2015, 17:36 UTC
- Hora da edição: 18 de dezembro de 2018, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : "arn:aws:execute-api:*:*:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonAPIGatewayPushToCloudWatchLogs

Descrição: permite que o API Gateway envie logs por push para a conta do usuário.

`AmazonAPIGatewayPushToCloudWatchLogs` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonAPIGatewayPushToCloudWatchLogs` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 11 de novembro de 2015, 23:41 UTC
- Hora da edição: 11 de novembro de 2015, 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:FilterLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonAppFlowFullAccess

Descrição: Fornece acesso total à Amazon AppFlow e acesso aos AWS serviços suportados como origem ou destino do fluxo (S3 e Redshift). Também fornece acesso ao KMS para criptografia

`AmazonAppFlowFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonAppFlowFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 02 de junho de 2020, 23:30 UTC

- Hora da edição: 28 de fevereiro de 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "appflow:*",
      "Resource" : "*"
    },
    {
      "Sid" : "ListRolesForRedshift",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "KMSListGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3PutBucketPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::appflow-*"
    },
    {
```

```
      "Sid" : "SecretsManagerCreateSecretAccess",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "appflow!*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPutResourcePolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        },
        "StringEqualsIgnoreCase" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appflow"
        }
      }
    },
    {
      "Sid" : "LambdaListFunctions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonAppFlowReadOnlyAccess

Descrição: fornece acesso somente leitura a fluxos do Amazon Appflow.

`AmazonAppFlowReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonAppFlowReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 02 de junho de 2020, 23:26 UTC
- Hora da edição: 28 de fevereiro de 2022, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnector",
        "appflow:DescribeConnectors",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlows",
        "appflow:DescribeFlowExecution",
        "appflow:DescribeConnectorFields",
        "appflow:ListConnectors",
        "appflow:ListConnectorFields",
        "appflow:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy

Descrição: Concede permissões ao switch de região ARC para execução e avaliação do plano.

`AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Horário de criação: 03 de novembro de 2025, 19:34 UTC
- Horário editado: 02 de outubro de 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "arc-region-switch:GetPlan",
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:ListPlanExecutions"
      ],
      "Resource" : "*",
      "Sid" : "GetPlanAndExecutions"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:SimulatePrincipalPolicy",
      "Resource" : "arn:aws:iam::*:role/*",
      "Sid" : "PlanEvaluation"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:GetMetricStatistics"
```

```
      ],
      "Resource" : "*",
      "Sid" : "CloudWatch"
    },
    {
      "Sid" : "ServiceQuotasRead",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceQuotasWrite",
      "Effect" : "Allow",
      "Action" : "servicequotas:RequestServiceQuotaIncrease",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonAppStreamFullAccess

Descrição: Fornece acesso total à Amazon AppStream por meio do Console de gerenciamento da AWS.

`AmazonAppStreamFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonAppStreamFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 28 de agosto de 2020, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamFullAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "appstream:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
```

```
        "application-autoscaling:DeleteScheduledAction"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "iam:ListRoles",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/service-role/
ApplicationAutoScalingForAmazonAppStreamAccess",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appstream.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_AppStreamFleet",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "appstream.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonAppStreamPCAAccess

Descrição: Acesso da Amazon AppStream 2.0 à CA privada do AWS Certificate Manager em contas de clientes para autenticação baseada em certificados

`AmazonAppStreamPCAAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonAppStreamPCAAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 24 de outubro de 2022, 17:05 UTC
- Hora da edição: 24 de outubro de 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:*:acm-pca:*:*:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/euc-private-ca" : "*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonAppStreamReadOnlyAccess

Descrição: Fornece acesso somente para leitura à Amazon AppStream por meio do Console de gerenciamento da AWS.

`AmazonAppStreamReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonAppStreamReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:List*",
        "appstream:Describe*"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonAppStreamServiceAccess

Descrição: Política padrão para a função AppStream de serviço da Amazon.

`AmazonAppStreamServiceAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonAppStreamServiceAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 19 de novembro de 2016, 4:17 UTC
- Horário editado: 03 de setembro de 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints",
        "s3:ListAllMyBuckets",
        "ds:DescribeDirectories",
        "application-autoscaling:DescribeScalableTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::appstream2-36fb080bb8-*",
        "arn:aws:s3:::appstream-app-settings-*",
```

```
        "arn:aws:s3:::appstream-logs-*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonAthenaFullAccess

Descrição: fornece acesso total ao Amazon Athena e acesso limitado às dependências necessárias para permitir a consulta, a gravação de resultados e o gerenciamento de dados.

`AmazonAthenaFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonAthenaFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de novembro de 2016, 16:46 UTC
- Horário editado: 12 de fevereiro de 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAthenaFullAccess`

Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseAthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseGluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:StartColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
```

```
        "glue:GetCatalogImportStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseQueryResultsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-athena-query-results-*"
      ]
    },
    {
      "Sid" : "BaseAthenaExamplesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::athena-examples*"
      ]
    },
    {
      "Sid" : "BaseS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "BaseSNSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseCloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseDataZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:ListDomains",
        "datazone:ListProjects",
        "datazone:ListAccountEnvironments"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BasePricingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonAthenaServiceRolePolicy

Descrição: Permite o acesso a outros recursos AWS de serviço necessários para executar o Amazon Athena

`AmazonAthenaServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 14 de novembro de 2025, 22:34 UTC
- Horário editado: 14 de novembro de 2025, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonAthenaServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Athena",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonAugmentedAIFullAccess

Descrição: Fornece acesso para realizar todas as operações dos recursos de IA aumentada da Amazon FlowDefinitions, incluindo HumanTaskUis e. HumanLoops Não permite acesso para criar FlowDefinitions contra o público Workteam.

`AmazonAugmentedAIFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonAugmentedAIFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 03 de dezembro de 2019, 16:21 UTC
- Hora da edição: 03 de dezembro de 2019, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops",
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions",
        "sagemaker:*HumanTaskUi",
        "sagemaker:*HumanTaskUis"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonAugmentedAIHumanLoopFullAccess

Descrição: Fornece acesso para realizar todas as operações em HumanLoops.

`AmazonAugmentedAIHumanLoopFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonAugmentedAIHumanLoopFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 03 de dezembro de 2019, 16:20 UTC
- Hora da edição: 03 de dezembro de 2019, 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonAugmentedAIIntegratedAPIAccess

Descrição: Fornece acesso para realizar todas as operações dos recursos de IA aumentada da Amazon FlowDefinitions, incluindo HumanTaskUis e. HumanLoops Também fornece acesso às operações de serviços que são integradas com o Amazon Augmented AI.

`AmazonAugmentedAIIntegratedAPIAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonAugmentedAIIntegratedAPIAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 22 de abril de 2020, 20:47 UTC
- Hora da edição: 22 de abril de 2020, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops",
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions",
        "sagemaker:*HumanTaskUi",
        "sagemaker:*HumanTaskUis"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "textract:AnalyzeDocument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:DetectModerationLabels"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonAuroraDSQLConsoleFullAccess

Descrição: concede acesso administrativo completo do console ao Aurora DSQL

`AmazonAuroraDSQLConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonAuroraDSQLConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de dezembro de 2024, 15:36 UTC
- Horário editado: 13 de maio de 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLConsoleFullAccess`

Versão da política

Versão da política: v16 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DsqlAllPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:PutClusterPolicy",
        "dsql:GetClusterPolicy",
        "dsql:DeleteClusterPolicy",
        "dsql:CreateCluster",
        "dsql:GetCluster",
        "dsql:UpdateCluster",
        "dsql:DeleteCluster",
        "dsql:ListClusters",
        "dsql:TagResource",
        "dsql:UntagResource",
        "dsql:ListTagsForResource",
        "dsql:DbConnectAdmin",
        "dsql:DbConnect",
        "dsql:PutMultiRegionProperties",
        "dsql:PutWitnessRegion",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:InjectError",
        "dsql:CreateStream",
```

```
        "dsql:DeleteStream",
        "dsql:GetStream",
        "dsql:ListStreams",
        "dsql:UpdateStream"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DsqlConsolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ValidatePolicy",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "cloudwatch:GetMetricData",
        "ec2:DescribeVpcEndpoints",
        "kms:ListAliases",
        "kms:DescribeKey",
        "cloudwatch:ListMetrics",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSCryptographicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
        }
```

```
      }
    },
    {
      "Sid" : "CreateDsqlServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "dsql.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassRoleForChangeStreams",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "dsql.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonAuroraDSQLFullAccess

Descrição: concede acesso administrativo completo ao Aurora DSQL

`AmazonAuroraDSQLFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonAuroraDSQLFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de dezembro de 2024, 15:36 UTC
- Horário editado: 13 de maio de 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLFullAccess`

Versão da política

Versão da política: v16 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DsqlAllPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:PutClusterPolicy",
        "dsql:GetClusterPolicy",
        "dsql:DeleteClusterPolicy",
        "dsql:CreateCluster",
        "dsql:GetCluster",
        "dsql:UpdateCluster",
        "dsql:DeleteCluster",
        "dsql:ListClusters",
        "dsql:TagResource",
        "dsql:UntagResource",
        "dsql:ListTagsForResource",
        "dsql:DbConnectAdmin",
```

```
        "dsql:DbConnect",
        "dsql:PutMultiRegionProperties",
        "dsql:PutWitnessRegion",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:InjectError",
        "dsql:CreateStream",
        "dsql:DeleteStream",
        "dsql:GetStream",
        "dsql:ListStreams",
        "dsql:UpdateStream"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedServicesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDsqlServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "dsql.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KMSDescribePermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForChangeStreams",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "dsql.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KMSCryptographicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
        }
      }
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonAuroraDSQLReadOnlyAccess

Descrição: fornece acesso somente leitura ao Aurora DSQL.

`AmazonAuroraDSQLReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonAuroraDSQLReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de dezembro de 2024, 15:21 UTC
- Horário editado: 13 de maio de 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLReadOnlyAccess`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DsqlReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetClusterPolicy",
        "dsql:GetCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dsql:GetStream",
        "dsql:ListStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedServicesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRo

Descrição: concede permissão de inferência do modelo do Bedrock para a memória principal do atendente do Bedrock

`AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 16 de julho de 2025, 13:37 UTC
- Horário editado: 17 de julho de 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockInvokeModel",
```

```
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockMantleInference",
      "Effect" : "Allow",
      "Action" : "bedrock-mantle:CreateInference",
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
      "Action" : "bedrock-mantle:CallWithBearerToken",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBedrockExternalWebSearchFullAccess

Descrição: Fornece acesso total ao Amazon Bedrock Web Search, incluindo a recuperação de conteúdo de sites externos fora dos limites da rede. AWS

`AmazonBedrockExternalWebSearchFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonBedrockExternalWebSearchFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de agosto de 2026, 16:57 UTC
- Horário editado: 03 de agosto de 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockExternalWebSearchFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockExternalWebSearchFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch",
```

```
        "bedrock-websearch:ExternalWebAccess"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBedrockExternalWebSearchReadOnly

Descrição: Fornece acesso somente para leitura ao Amazon Bedrock Web Search, incluindo a recuperação de conteúdo de sites externos fora dos limites da rede. AWS

`AmazonBedrockExternalWebSearchReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonBedrockExternalWebSearchReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de agosto de 2026, 16:57 UTC
- Horário editado: 03 de agosto de 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockExternalWebSearchReadOnly`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockExternalWebSearchReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch",
        "bedrock-websearch:ExternalWebAccess"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBedrockFullAccess

Descrição: fornece acesso total ao Amazon Bedrock, bem como acesso limitado aos serviços relacionados exigidos por ele

`AmazonBedrockFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonBedrockFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 6 de dezembro de 2023, 15:47 UTC
- Horário editado: 04 de agosto de 2026, 05:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockFullAccess`

Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockMantleAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockWebSearch",
      "Effect" : "Allow",
      "Action" : [
```

```
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    },
    {
      "Sid" : "DescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:*:kms:*:::*"
    },
    {
      "Sid" : "APIsWithAllResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceModelEndpointMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
```

```
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointAddTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:RequestTag/bedrock:marketplace-registration-status" : "registered",
          "aws:RequestTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointDeleteTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
```

```
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:ResourceTag/bedrock:marketplace-registration-status" : "registered",
          "aws:ResourceTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointNonMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:ListEndpoints",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointInvokingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
      }
    },
    {
      "Sid" : "DiscoveringMarketplaceModel",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*",
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
    {
      "Sid" : "AllowMarketplaceModelsListing",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListHubContents"
      ],
      "Resource" : "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
    },
    {
      "Sid" : "PassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*ForBedrock*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "PassRoleToBedrock",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonBedrock*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrockFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBedrockLimitedAccess

Descrição: fornece acesso limitado ao Amazon Bedrock e aos serviços relacionados exigidos por ele.

`AmazonBedrockLimitedAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonBedrockLimitedAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 29 de junho de 2025, 22:22 UTC
- Horário editado: 04 de agosto de 2026, 05:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockLimitedAccess`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:Get*",
        "bedrock:List*",
        "bedrock:CallWithBearerToken",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:CancelAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:CreateAutomatedReasoningPolicy",
```

```
        "bedrock:CreateAutomatedReasoningPolicyTestCase",
        "bedrock:CreateAutomatedReasoningPolicyVersion",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreateGuardrail",
        "bedrock:CreateGuardrailVersion",
        "bedrock:CreateInferenceProfile",
        "bedrock:CreateModelCopyJob",
        "bedrock:CreateModelCustomizationJob",
        "bedrock:CreateModelImportJob",
        "bedrock:CreateModelInvocationJob",
        "bedrock:CreatePromptRouter",
        "bedrock:CreateProvisionedModelThroughput",
        "bedrock:DeleteAutomatedReasoningPolicy",
        "bedrock:DeleteAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:DeleteAutomatedReasoningPolicyTestCase",
        "bedrock:DeleteCustomModel",
        "bedrock:DeleteGuardrail",
        "bedrock:DeleteImportedModel",
        "bedrock:DeleteInferenceProfile",
        "bedrock:DeletePromptRouter",
        "bedrock:DeleteProvisionedModelThroughput",
        "bedrock:ExportAutomatedReasoningPolicyVersion",
        "bedrock:StartAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:StartAutomatedReasoningPolicyTestWorkflow",
        "bedrock:StopEvaluationJob",
        "bedrock:StopModelCustomizationJob",
        "bedrock:StopModelInvocationJob",
        "bedrock:TagResource",
        "bedrock:UntagResource",
        "bedrock:UpdateAutomatedReasoningPolicy",
        "bedrock:UpdateAutomatedReasoningPolicyAnnotations",
        "bedrock:UpdateAutomatedReasoningPolicyTestCase",
        "bedrock:UpdateGuardrail",
        "bedrock:UpdateProvisionedModelThroughput",
        "bedrock:ApplyGuardrail",
        "bedrock:InvokeAutomatedReasoningPolicy",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeKey",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:*:kms:*:::*"
    },
    {
      "Sid" : "APIsWithAllResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockMantleAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:Get*",
        "bedrock-mantle:List*",
        "bedrock-mantle:CreateInference"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockWebSearch",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrockFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "bedrock.amazonaws.com",
            "bedrock-mantle.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBedrockMantleFullAccess

Descrição: Fornece acesso total ao Amazon Bedrock Mantle, bem como acesso limitado aos serviços relacionados que são exigidos por ele

`AmazonBedrockMantleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonBedrockMantleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Tempo de criação: 04 de dezembro de 2025, 07:19 UTC
- Horário editado: 04 de agosto de 2026, 04:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleFullAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMantleAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockWebSearch",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrockMantleFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock-mantle.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBedrockMantleInferenceAccess

Descrição: Fornece acesso de leitura e criação de inferências ao Amazon Bedrock Mantle

`AmazonBedrockMantleInferenceAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonBedrockMantleInferenceAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Tempo de criação: 04 de dezembro de 2025, 07:19 UTC
- Horário editado: 04 de agosto de 2026, 05:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleInferenceAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMantleInference",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:Get*",
        "bedrock-mantle:List*",
        "bedrock-mantle:CreateInference"
      ],
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*"
    },
    {
      "Sid" : "BedrockWebSearch",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    },
    {
      "Sid" : "BedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:CallWithBearerToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrockMantleFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock-mantle.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBedrockMantleReadOnly

Descrição: Fornece acesso somente para leitura ao Amazon Bedrock Mantle

`AmazonBedrockMantleReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonBedrockMantleReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Tempo de criação: 04 de dezembro de 2025, 07:19 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleReadOnly`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMantleReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:Get*",
        "bedrock-mantle:List*"
      ],
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*"
    },
    {
      "Sid" : "BedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:CallWithBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBedrockMarketplaceAccess

Descrição: fornece acesso limitado ao Amazon Bedrock Marketplace e aos serviços relacionados exigidos por ele.

`AmazonBedrockMarketplaceAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonBedrockMarketplaceAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 29 de junho de 2025, 22:22 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMarketplaceAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMarketplaceAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateMarketplaceModelEndpoint",
        "bedrock:DeleteMarketplaceModelEndpoint",
        "bedrock:DeregisterMarketplaceModelEndpoint",
        "bedrock:RegisterMarketplaceModelEndpoint",
        "bedrock:UpdateMarketplaceModelEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceModelEndpointMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointAddTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:RequestTag/bedrock:marketplace-registration-status" : "registered",
          "aws:RequestTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
```

```
    },
    {
      "Sid" : "MarketplaceModelEndpointDeleteTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:ResourceTag/bedrock:marketplace-registration-status" : "registered",
          "aws:ResourceTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointNonMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:ListEndpoints",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointInvokingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
      }
    },
    {
      "Sid" : "DiscoveringMarketplaceModel",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*",
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
    {
      "Sid" : "AllowMarketplaceModelsListing",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListHubContents"
      ],
      "Resource" : "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
    },
    {
      "Sid" : "PassRoleToSageMaker",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*ForBedrock*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleToBedrock",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonBedrock*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBedrockReadOnly

Descrição: fornece acesso somente leitura ao Amazon Bedrock

`AmazonBedrockReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonBedrockReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 6 de dezembro de 2023, 15:48 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockReadOnly`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:Get*",
        "bedrock:List*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "MarketplaceModelEndpointNonMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:ListEndpoints",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DiscoveringMarketplaceModel",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*",
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
    {
      "Sid" : "AllowMarketplaceModelsListing",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListHubContents"
      ],
      "Resource" : "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBedrockStudioPermissionsBoundary

Descrição: define as permissões máximas dos perfis do IAM que o Amazon Bedrock Studio cria para operar os recursos do Amazon Bedrock Studio.

`AmazonBedrockStudioPermissionsBoundary` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonBedrockStudioPermissionsBoundary` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 1º de agosto de 2024, 0:24 UTC
- Hora da edição: 1º de agosto de 2024, 0:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockStudioPermissionsBoundary`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "AccessS3Buckets",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:ListBucketVersions",
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject",
      "s3:GetObjectVersion",
      "s3:DeleteObjectVersion"
    ],
    "Resource" : "arn:aws:s3:::br-studio-${aws:PrincipalAccount}-*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "AccessOpenSearchCollections",
    "Effect" : "Allow",
    "Action" : "aoss:APIAccessAll",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "InvokeBedrockModels",
    "Effect" : "Allow",
    "Action" : [
      "bedrock:InvokeModel",
      "bedrock:InvokeModelWithResponseStream"
    ],
    "Resource" : "arn:aws:bedrock:*::foundation-model/*"
  },
  {
    "Sid" : "AccessBedrockResources",
    "Effect" : "Allow",
```

```
      "Action" : [
        "bedrock:InvokeAgent",
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
        "bedrock:ListIngestionJobs",
        "bedrock:ApplyGuardrail",
        "bedrock:ListPrompts",
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
        "bedrock:ListTagsForResource",
        "bedrock:TagResource",
        "bedrock:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RetrieveAndGenerate",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "WriteLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/br-studio-*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "InvokeLambdaFunctions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:br-studio-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AccessSecretsManagerSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:br-studio/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "UseKmsKeyWithBedrock",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/EnableBedrock" : "true"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
        }
      }
    },
    {
      "Sid" : "UseKmsKeyWithAwsServices",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/EnableBedrock" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBedrockWebSearchFullAccess

Descrição: Fornece acesso total ao Amazon Bedrock Web Search. Os dados permanecem dentro dos limites AWS da rede.

`AmazonBedrockWebSearchFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonBedrockWebSearchFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de agosto de 2026, 16:42 UTC
- Horário editado: 03 de agosto de 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockWebSearchFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockWebSearchFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBedrockWebSearchReadOnly

Descrição: Fornece acesso somente para leitura ao Amazon Bedrock Web Search. Os dados permanecem dentro dos limites AWS da rede.

`AmazonBedrockWebSearchReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonBedrockWebSearchReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de agosto de 2026, 16:57 UTC
- Horário editado: 03 de agosto de 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockWebSearchReadOnly`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockWebSearchReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-websearch:InvokeSearch",
        "bedrock-websearch:InvokeFetch"
      ],
      "Resource" : "arn:aws:bedrock-websearch:*:*:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBioDiscoveryFullAccess

Descrição: Permite acesso administrativo total ao Amazon Bio Discovery

`AmazonBioDiscoveryFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonBioDiscoveryFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 18 de agosto de 2026, 06:27 UTC
- Horário editado: 18 de agosto de 2026, 06:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBioDiscoveryFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBioDiscoveryFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "researchstudio:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonBioDiscoveryPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : "researchstudio.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonBioDiscoveryIdentityStoreAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser"
      ],
      "Resource" : [
        "arn:aws:identitystore::*:identitystore/*",
        "arn:aws:identitystore:::user/*",
        "arn:aws:identitystore:::group/*",
        "arn:aws:identitystore:::membership/*"
      ]
    },
    {
      "Sid" : "AmazonBioDiscoveryIdentityCenterAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplication",
        "sso:DeleteApplicationAuthenticationMethod",
        "sso:DeleteApplicationGrant",
        "sso:DescribeApplication",
        "sso:DescribeApplicationAssignment",
        "sso:GetApplicationAuthenticationMethod",
        "sso:GetApplicationGrant",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant",
        "sso:DeleteApplicationAssignment",
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso:ListApplications",
        "sso:ListApplicationAssignments",
        "sso:ListApplicationGrants",
        "sso:PutApplicationAccessScope",
```

```
        "sso:DeleteApplicationAccessScope",
        "sso:ListApplicationAccessScopes",
        "sso:DescribeRegisteredRegions"
      ],
      "Resource" : [
        "arn:aws:sso:::instance/*",
        "arn:aws:sso::*:application/*/*",
        "arn:aws:sso::aws:applicationProvider/ResearchStudio"
      ]
    },
    {
      "Sid" : "AmazonBioDiscoveryIdentityCenterKMSAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:aws:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonBioDiscoveryIdentityStoreKMSAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:aws:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBioDiscoveryInAppFullAccess

Descrição: Fornece acesso total às ações nos aplicativos Amazon Bio Discovery

`AmazonBioDiscoveryInAppFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonBioDiscoveryInAppFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 18 de agosto de 2026, 06:47 UTC
- Horário editado: 18 de agosto de 2026, 06:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBioDiscoveryInAppFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBioDiscoveryInAppFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "researchstudio:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonBioDiscoveryIdentityStoreInAppAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "arn:aws:identitystore::*:identitystore/*",
        "arn:aws:identitystore:::user/*",
        "arn:aws:identitystore:::group/*",
        "arn:aws:identitystore:::membership/*"
      ]
    },
    {
      "Sid" : "AmazonBioDiscoveryIdentityCenterInAppAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplicationAssignment",
        "sso:ListApplicationAssignments"
      ],
      "Resource" : [
        "arn:aws:sso:::instance/*",
        "arn:aws:sso::*:application/*/*"
      ]
    },
    {
      "Sid" : "AmazonBioDiscoveryIdentityCenterKMSInAppAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:aws:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonBioDiscoveryIdentityStoreKMSInAppAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:aws:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBraketFullAccess

Descrição: Fornece acesso total ao Amazon Braket por meio do SDK Console de gerenciamento da AWS e. Também fornece acesso a serviços relacionados (por exemplo, S3, registros).

`AmazonBraketFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonBraketFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de agosto de 2020, 20:12 UTC
- Horário editado: 06 de julho de 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

Versão da política

Versão da política: v13 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
```

```
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/AmazonBraket" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "servicequotas:GetServiceQuota",
        "cloudwatch:GetMetricData",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability"
```

```
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/amazon-braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListNotebookInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StopNotebookInstance",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:ListTags",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance/amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/amazon-
braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "braket:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/braket.amazonaws.com/
AWSServiceRoleForAmazonBraket*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "braket.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonBraketServiceSageMakerNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonBraketJobsExecutionRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "braket.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "/aws/braket"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBraketJobsExecutionPolicy

Descrição: Concede acesso Serviços da AWS e recursos necessários para executar um trabalho do Amazon Braket, incluindo S3, Cloudwatch, IAM e Braket

`AmazonBraketJobsExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonBraketJobsExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de novembro de 2021, 19:34 UTC
- Horário editado: 06 de julho de 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/AmazonBraket" : "true"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/amazon-braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "braket:CancelJob",
        "braket:CancelQuantumTask",
        "braket:CreateJob",
        "braket:CreateQuantumTask",
        "braket:GetDevice",
        "braket:GetJob",
        "braket:GetQuantumTask",
        "braket:SearchDevices",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "braket:ListTagsForResource",
        "braket:TagResource",
        "braket:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonBraketJobsExecutionRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "braket.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:GetLogEvents",
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:StopQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "/aws/braket"
        }
      }
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonBraketServiceRolePolicy

Descrição: permite que o Amazon Braket crie e gerencie AWS recursos em seu nome

`AmazonBraketServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 04 de agosto de 2020, 17:12 UTC
- Horário editado: 06 de julho de 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/AmazonBraket" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
```

```
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonChimeFullAccess

Descrição: fornece acesso total ao console de administração do Amazon Chime via Console de gerenciamento da AWS.

`AmazonChimeFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonChimeFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de novembro de 2017, 22:15 UTC
- Hora da edição: 14 de dezembro de 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:CreateQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Action" : [
        "kinesis:ListStreams"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/chime-chat-*",
        "arn:aws:kinesis:*:*:stream/chime-messaging-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration",
        "s3:ListBucket"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::chime-chat-*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonChimeReadOnly

Descrição: fornece acesso somente leitura ao console de administração do Amazon Chime via Console de gerenciamento da AWS.

`AmazonChimeReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonChimeReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de novembro de 2017, 22:04 UTC
- Hora da edição: 14 de dezembro de 2020, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:List*",
        "chime:Get*",
        "chime:Describe*",
        "chime:SearchAvailablePhoneNumbers"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonChimeSDK

Descrição: fornece acesso total a operações do SDK do Amazon Chime.

`AmazonChimeSDK` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonChimeSDK` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 04 de fevereiro de 2020, 21:53 UTC

- Hora da edição: 10 de janeiro de 2023, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeSDK`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:CreateMeeting",
        "chime:CreateMeetingWithAttendees",
        "chime:DeleteMeeting",
        "chime:GetMeeting",
        "chime:ListMeetings",
        "chime:CreateAttendee",
        "chime:BatchCreateAttendee",
        "chime:DeleteAttendee",
        "chime:GetAttendee",
        "chime:ListAttendees",
        "chime:ListAttendeeTags",
        "chime:ListMeetingTags",
        "chime:ListTagsForResource",
        "chime:TagAttendee",
        "chime:TagMeeting",
        "chime:TagResource",
        "chime:UntagAttendee",
        "chime:UntagMeeting",
        "chime:UntagResource",
        "chime:StartMeetingTranscription",
        "chime:StopMeetingTranscription",
        "chime:CreateMediaCapturePipeline",
```

```
        "chime:CreateMediaConcatenationPipeline",
        "chime:CreateMediaLiveConnectorPipeline",
        "chime:DeleteMediaCapturePipeline",
        "chime:DeleteMediaPipeline",
        "chime:GetMediaCapturePipeline",
        "chime:GetMediaPipeline",
        "chime:ListMediaCapturePipelines",
        "chime:ListMediaPipelines"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

Descrição: Política gerenciada para a função vinculada ao MediaPipelines serviço Amazon Chime SDK

`AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 04 de abril de 2022, 22:02 UTC

- Hora da edição: 8 de dezembro de 2023, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutMetricsForChimeSDKNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ChimeSDK"
        }
      }
    },
    {
      "Sid" : "AllowKinesisVideoStreamsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:UpdateDataRetention",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/ChimeMediaPipelines-*"
      ]
```

```
    },
    {
      "Sid" : "AllowKinesisVideoStreamsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowChimeMeetingAccess",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetMeeting",
        "chime:CreateAttendee",
        "chime:DeleteAttendee"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonChimeSDKMessagingServiceRolePolicy

Descrição: permite que o Amazon Chime SDK Messaging acesse AWS recursos e habilite a funcionalidade de mensagens

`AmazonChimeSDKMessagingServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 03 de março de 2023, 1:43 UTC
- Hora da edição: 03 de março de 2023, 1:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "kinesis.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
```

```
        "kinesis:DescribeStream"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/chime-messaging-*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonChimeServiceRolePolicy

Descrição: Permite o acesso aos AWS recursos usados ou gerenciados pelo Amazon Chime

`AmazonChimeServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 30 de setembro de 2019, 22:25 UTC
- Hora da edição: 30 de setembro de 2019, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/chime.amazonaws.com/
AWSServiceRoleForAmazonChime"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "chime.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonChimeTranscriptionServiceLinkedRolePolicy

Descrição: permite que o Amazon Chime acesse o Amazon Transcribe e o Amazon Transcribe Medical em seu nome

`AmazonChimeTranscriptionServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 04 de agosto de 2021, 21:47 UTC
- Hora da edição: 04 de agosto de 2021, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:StartStreamTranscription",
        "transcribe:StartMedicalStreamTranscription"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonChimeUserManagement

Descrição: fornece acesso de gerenciamento de usuários ao console de administração do Amazon Chime via Console de gerenciamento da AWS.

`AmazonChimeUserManagement` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonChimeUserManagement` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de novembro de 2017, 22:17 UTC
- Hora da edição: 18 de fevereiro de 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeUserManagement`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
```

```
        "chime:ListAccounts",
        "chime:GetAccount",
        "chime:GetAccountSettings",
        "chime:UpdateAccountSettings",
        "chime:ListUsers",
        "chime:GetUser",
        "chime:GetUserByEmail",
        "chime:InviteUsers",
        "chime:InviteUsersFromProvider",
        "chime:SuspendUsers",
        "chime:ActivateUsers",
        "chime:UpdateUserLicenses",
        "chime:ResetPersonalPIN",
        "chime:LogoutUser",
        "chime:ListDomains",
        "chime:GetDomain",
        "chime:ListDirectories",
        "chime:ListGroups",
        "chime:SubmitSupportRequest",
        "chime:ListDelegates",
        "chime:ListAccountUsageReportData",
        "chime:GetMeetingDetail",
        "chime:ListMeetingEvents",
        "chime:ListMeetingsReportData",
        "chime:GetUserActivityReportData",
        "chime:UpdateUser",
        "chime:BatchUpdateUser",
        "chime:BatchSuspendUser",
        "chime:BatchUnsuspendUser",
        "chime:AssociatePhoneNumberWithUser",
        "chime:DisassociatePhoneNumberFromUser",
        "chime:GetPhoneNumber",
        "chime:ListPhoneNumbers",
        "chime:GetUserSettings",
        "chime:UpdateUserSettings",
        "chime:CreateUser",
        "chime:AssociateSigninDelegateGroupsWithAccount",
        "chime:DisassociateSigninDelegateGroupsFromAccount"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

Descrição: Política gerenciada para Service Linked Role for Amazon Chime VoiceConnector

`AmazonChimeVoiceConnectorServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 30 de setembro de 2019, 22:16 UTC
- Hora da edição: 14 de abril de 2023, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:GetVoiceConnector*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:UpdateDataRetention",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/ChimeVoiceConnector-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:CreateMediaInsightsPipeline",
        "chime:GetMediaInsightsPipelineConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCloudDirectoryFullAccess

Descrição: fornece acesso total ao Amazon Cloud Directory Service.

`AmazonCloudDirectoryFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCloudDirectoryFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de fevereiro de 2017, 0:41 UTC
- Hora da edição: 25 de fevereiro de 2017, 0:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "clouddirectory:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCloudDirectoryReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon Cloud Directory Service.

`AmazonCloudDirectoryReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCloudDirectoryReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de fevereiro de 2017, 23:42 UTC
- Hora da edição: 28 de fevereiro de 2017, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "clouddirectory:List*",
        "clouddirectory:Get*",
        "clouddirectory:LookupPolicy",
        "clouddirectory:BatchRead"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCloudWatchEvidentlyFullAccess

Descrição: Fornece acesso completo somente à Amazon CloudWatch Evidently. Também fornece acesso ao Amazon S3, Amazon SNS CloudWatch, Amazon e outros serviços relacionados.

`AmazonCloudWatchEvidentlyFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCloudWatchEvidentlyFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2021,15:10 UTC

- Hora da edição: 29 de novembro de 2021, 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "evidently:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchRUMEvidentlyRole-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:TagResource",
        "cloudwatch:UnTagResource"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:Evidently-Alarm-*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "arn:*:sns:*:*:Evidently-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCloudWatchEvidentlyReadOnlyAccess

Descrição: Fornece acesso somente para leitura à Amazon CloudWatch Evidently

`AmazonCloudWatchEvidentlyReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCloudWatchEvidentlyReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2021,15:08 UTC
- Hora da edição: 29 de novembro de 2021, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "evidently:GetExperiment",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCloudWatchEvidentlyServiceRolePolicy

Descrição: permite que o CloudWatch Evidently Service gerencie AWS os recursos associados em nome do cliente

`AmazonCloudWatchEvidentlyServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 13 de setembro de 2022, 17:25 UTC
- Hora da edição: 13 de setembro de 2022, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "appconfig:StartDeployment",
      "Resource" : [
        "arn:aws:appconfig:*:*:application/*",
        "arn:aws:appconfig:*:*:deploymentstrategy/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "appconfig:StartDeployment",
      "Resource" : "arn:aws:appconfig:*:*:application/*/configurationprofile/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/Owner" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "appconfig:TagResource",
      "Resource" : "arn:aws:appconfig:*:*:application/*/environment/*/deployment/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "appconfig:StopDeployment",
      "Resource" : "arn:aws:appconfig:*:*:application/*"
    },
    {
      "Effect" : "Deny",
      "Action" : "appconfig:StopDeployment",
      "Resource" : "arn:aws:appconfig:*:*:application/*/environment/*/deployment/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "appconfig:ListDeployments",
      "Resource" : "arn:aws:appconfig:*:*:application/*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCloudWatchRUMFullAccess

Descrição: Concede permissões de acesso total ao serviço Amazon CloudWatch RUM

`AmazonCloudWatchRUMFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCloudWatchRUMFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2021,15:46 UTC

- Hora da edição: 29 de novembro de 2021, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/rum.amazonaws.com/
AWSServiceRoleForRealUserMonitoring"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/RUM-Monitor*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:CreateIdentityPool",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:SetIdentityPoolRoles"
      ],
      "Resource" : "arn:aws:cognito-identity:*:*:identitypool/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy",
        "logs:CreateLogStream"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*RUMService*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group::log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:describeCanaries",
        "synthetics:describeCanariesLastRun"
      ],
      "Resource" : "arn:aws:synthetics:*:*:canary:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCloudWatchRUMReadOnlyAccess

Descrição: Concede permissões somente de leitura para o serviço Amazon CloudWatch RUM

`AmazonCloudWatchRUMReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCloudWatchRUMReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2021,15:43 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListRumMetricsDestinations",
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetResourcePolicy",
        "rum:ListTagsForResource"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:describeCanariesLastRun",
        "synthetics:describeCanaries"
      ],
      "Resource" : "arn:aws:synthetics:*:*:canary:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group::log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCloudWatchRUMServiceRolePolicy

Descrição: Concede permissão ao Amazon CloudWatch RUM Service para publicar dados de monitoramento em outros AWS serviços relevantes

`AmazonCloudWatchRUMServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 17 de novembro de 2021, 23:17 UTC
- Hora da edição: 22 de fevereiro de 2023, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "RUM/CustomMetrics/*",
            "AWS/RUM"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCodeCatalystFullAccess

Descrição: Fornece acesso total à Amazon CodeCatalyst

`AmazonCodeCatalystFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCodeCatalystFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 20 de abril de 2023, 16:50 UTC
- Hora da edição: 20 de abril de 2023, 16:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeCatalystResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecatalyst:*",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCatalystAssociateIAMRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "codecatalyst.amazonaws.com",
```

```
            "codecatalyst-runner.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCodeCatalystReadOnlyAccess

Descrição: Fornece acesso somente para leitura à Amazon CodeCatalyst

`AmazonCodeCatalystReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCodeCatalystReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 20 de abril de 2023, 16:49 UTC
- Hora da edição: 20 de abril de 2023, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecatalyst:Get*",
        "codecatalyst:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCodeCatalystSupportAccess

Descrição: Permite que CodeCatalyst a Amazon crie, atualize e resolva AWS Support casos em seu nome.

`AmazonCodeCatalystSupportAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCodeCatalystSupportAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 20 de abril de 2023, 12:34 UTC
- Hora da edição: 20 de abril de 2023, 12:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeAttachment",
        "support:DescribeCaseAttributes",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:DescribeIssueTypes",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeSupportLevel",
        "support:SearchForCases",
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:InitiateCallForCase",
        "support:InitiateChatForCase",
        "support:PutCaseAttributes",
        "support:RateCaseCommunication",
        "support:ResolveCase"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCodeGuruProfilerAgentAccess

Descrição: Fornece o acesso exigido pelo agente Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerAgentAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCodeGuruProfilerAgentAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 05 de fevereiro de 2021, 22:11 UTC
- Hora da edição: 05 de maio de 2022, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:ConfigureAgent",
        "codeguru-profiler:CreateProfilingGroup",
        "codeguru-profiler:PostAgentProfile"
      ],
      "Resource" : "arn:aws:codeguru-profiler:*:*:profilingGroup/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCodeGuruProfilerFullAccess

Descrição: Fornece acesso total ao Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCodeGuruProfilerFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 3 de dezembro de 2019, 10:13 UTC

- Hora da edição: 15 de julho de 2020, 3:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeguru-profiler:*",
        "iam:ListRoles",
        "iam:ListUsers",
        "sns:ListTopics",
        "codeguru:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/*AWSServiceRoleForCodeGuruProfiler*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "codeguru-profiler.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCodeGuruProfilerReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCodeGuruProfilerReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 3 de dezembro de 2019, 10:30 UTC
- Hora da edição: 27 de junho de 2020, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Action" : [
        "codeguru:Get*",
        "codeguru-profiler:BatchGet*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCodeGuruReviewerFullAccess

Descrição: Concede acesso total ao Amazon CodeGuru Reviewer e acesso limitado às dependências necessárias.

`AmazonCodeGuruReviewerFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCodeGuruReviewerFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 3 de dezembro de 2019, 8:33 UTC

- Hora da edição: 29 de agosto de 2020, 4:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:*",
        "codeguru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
```

```
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer"
    },
    {
      "Sid" : "CodeCommitAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCommitTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:TagResource",
        "codecommit:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "codeguru-reviewer"
        }
      }
    },
    {
      "Sid" : "CodeConnectTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "codeguru-reviewer"
        }
      }
    },
    {
      "Sid" : "CodeConnectManagedRules",
```

```
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codestar-connections:ListConnections",
        "codestar-connections:PassConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "codestar-connections:ProviderAction" : [
            "ListRepositories",
            "ListOwners"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCodeGuruReviewerReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon CodeGuru Reviewer.

`AmazonCodeGuruReviewerReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCodeGuruReviewerReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 3 de dezembro de 2019, 8:48 UTC
- Hora da edição: 29 de agosto de 2020, 4:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruReviewerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru:Get*",
        "codeguru-reviewer:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:Get*"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCodeGuruReviewerServiceRolePolicy

Descrição: É necessária uma função vinculada ao serviço para que o Amazon CodeGuru Reviewer acesse recursos em seu nome.

`AmazonCodeGuruReviewerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 3 de dezembro de 2019, 5:31 UTC
- Hora da edição: 27 de novembro de 2020, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessCodeGuruReviewerEnabledRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GetRepository",
        "codecommit:GetBranch",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetDifferences",
        "codecommit:GetPullRequest",
        "codecommit:ListPullRequests",
        "codecommit:PostCommentForPullRequest",
        "codecommit:GitPull",
        "codecommit:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/codeguru-reviewer" : "enabled"
        }
      }
    },
    {
      "Sid" : "AccessCodeGuruReviewerEnabledConnections",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "codestar-connections:ProviderAction" : [
            "ListBranches",
            "GetBranch",
```

```
            "ListRepositories",
            "ListOwners",
            "ListPullRequests",
            "GetPullRequest",
            "ListPullRequestComments",
            "ListPullRequestCommits",
            "ListCommitFiles",
            "ListBranchCommits",
            "CreatePullRequestDiffComment",
            "GitPull"
          ]
        },
        "Null" : {
          "aws:ResourceTag/codeguru-reviewer" : "false"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsResourceCleanup",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowGuruS3GetObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::codeguru-reviewer-*",
        "arn:aws:s3:::codeguru-reviewer-*/*"
      ]
    }
  ]
```

```
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCodeGuruSecurityFullAccess

Descrição: Fornece acesso total ao Amazon CodeGuru Security.

`AmazonCodeGuruSecurityFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCodeGuruSecurityFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de maio de 2023, 21:03 UTC
- Hora da edição: 09 de maio de 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruSecurityFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCodeGuruSecurityScanAccess

Descrição: Fornece o acesso necessário para trabalhar com escaneamentos CodeGuru de segurança da Amazon.

`AmazonCodeGuruSecurityScanAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCodeGuruSecurityScanAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de maio de 2023, 20:54 UTC
- Hora da edição: 09 de maio de 2023, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruSecurityScanAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:CreateUploadUrl",
        "codeguru-security:GetScan",
        "codeguru-security:GetFindings"
      ],
      "Resource" : "arn:aws:codeguru-security:*:*:scans/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCognitoDeveloperAuthenticatedIdentities

Descrição: fornece acesso às APIs do Amazon Cognito para oferecer suporte às identidades autenticadas do desenvolvedor a partir de seu backend de autenticação.

`AmazonCognitoDeveloperAuthenticatedIdentities` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCognitoDeveloperAuthenticatedIdentities` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de março de 2015, 17:22 UTC
- Hora da edição: 24 de março de 2015, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
        "cognito-identity:LookupDeveloperIdentity",
        "cognito-identity:MergeDeveloperIdentities",
        "cognito-identity:UnlinkDeveloperIdentity"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCognitoIdpEmailServiceRolePolicy

Descrição: permite que o serviço de grupos de usuários do Amazon Cognito use suas identidades do SES para enviar e-mails.

`AmazonCognitoIdpEmailServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 21 de março de 2019, 21:32 UTC
- Hora da edição: 21 de março de 2019, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ses:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCognitoIdpServiceRolePolicy

Descrição: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelos grupos de usuários do Amazon Cognito

`AmazonCognitoIdpServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 26 de junho de 2020, 22:30 UTC
- Hora da edição: 26 de junho de 2020, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCognitoPowerUser

Descrição: fornece acesso administrativo a recursos do Amazon Cognito. Você precisará de privilégios de Conta da AWS administrador para criar novos recursos do Cognito.

`AmazonCognitoPowerUser` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCognitoPowerUser` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de março de 2015, 17:14 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoPowerUser`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:*",
        "cognito-idp:*",
        "cognito-sync:*",
        "iam:ListRoles",
        "iam:ListOpenIdConnectProviders",
        "iam:GetRole",
```

```
        "iam:ListSAMLProviders",
        "iam:GetSAMLProvider",
        "kinesis:ListStreams",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "sns:GetSMSSandboxAccountStatus",
        "sns:ListPlatformApplications",
        "ses:ListIdentities",
        "ses:GetIdentityVerificationAttributes",
        "mobiletargeting:GetApps",
        "acm:ListCertificates",
        "sms-voice:DescribeAccountAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "cognito-idp.amazonaws.com",
            "email.cognito-idp.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/cognito-idp.amazonaws.com/
AWSServiceRoleForAmazonCognitoIdp*",
        "arn:aws:iam::*:role/aws-service-role/email.cognito-idp.amazonaws.com/
AWSServiceRoleForAmazonCognitoIdpEmail*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCognitoReadOnly

Descrição: fornece acesso somente leitura a recursos do Amazon Cognito.

`AmazonCognitoReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCognitoReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de março de 2015, 17:06 UTC
- Hora da edição: 01 de agosto de 2019, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoReadOnly`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:Describe*",
        "cognito-identity:Get*",
        "cognito-identity:List*",
        "cognito-idp:Describe*",
        "cognito-idp:AdminGet*",
        "cognito-idp:AdminList*",
        "cognito-idp:List*",
        "cognito-idp:Get*",
        "cognito-sync:Describe*",
        "cognito-sync:Get*",
        "cognito-sync:List*",
        "iam:ListOpenIdConnectProviders",
        "iam:ListRoles",
        "sns:ListPlatformApplications"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCognitoUnAuthedIdentitiesSessionPolicy

Descrição: esta política define o conjunto de permissões permitidas para identidades não autenticadas para o banco de identidades do Cognito. Esta política não se destina a ser usada como uma política de permissão independente. Ela é utilizada como uma barreira de proteção contra políticas excessivamente permissivas associadas a funções em um banco de identidades. Não vincule esta política a qualquer função, pois o Serviço de Identidade Cognito a incorporará automaticamente como uma política com escopo reduzido durante a criação de credenciais. Os privilégios para acessar temporariamente outros AWS recursos por meio do fluxo aprimorado agora

serão definidos pela interseção da função associada à identidade do usuário não autenticado fornecido por um serviço e pelos privilégios concedidos nessa política gerenciada de propriedade do Cognito.

`AmazonCognitoUnAuthedIdentitiesSessionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCognitoUnAuthedIdentitiesSessionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 19 de julho de 2023, 23:04 UTC
- Horário editado: 01 de maio de 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CognitoUnAuthedIdentitiesSessionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "rum:PutRumEvents",
        "sagemaker:InvokeEndpoint",
        "polly:*",
        "comprehend:*",
```

```
        "translate:*",
        "transcribe:*",
        "rekognition:*",
        "mobiletargeting:*",
        "firehose:*",
        "personalize:*",
        "geo:GetMap*",
        "geo:ListMaps",
        "geo:SearchPlaceIndex*",
        "geo:GetPlace",
        "geo:CalculateRoute*",
        "geo:*Geofence",
        "geo:*Geofences",
        "geo:*DevicePosition*",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyPair",
        "kms:GenerateDataKeyPairWithoutPlaintext",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonCognitoUnauthenticatedIdentities

Descrição: esta política define o conjunto de permissões permitidas para identidades não autenticadas para o banco de identidades do Cognito. Não vincule esta política a qualquer função, pois o Serviço de Identidade Cognito a incorporará automaticamente como uma política com escopo

reduzido durante a criação de credenciais. Os privilégios para acessar temporariamente outros AWS recursos por meio do fluxo aprimorado agora serão definidos pela interseção da função associada à identidade do usuário não autenticado fornecido por um serviço e pelos privilégios concedidos nessa política gerenciada de propriedade do Cognito.

`AmazonCognitoUnauthenticatedIdentities` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonCognitoUnauthenticatedIdentities` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de fevereiro de 2023, 22:36 UTC
- Hora da edição: 01 de fevereiro de 2023, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "rum:PutRumEvents",
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonConnect_FullAccess

Descrição: O objetivo desta política é conceder permissões aos usuários do AWS Connect que precisam usar os recursos do Connect. Essa política fornece acesso total aos recursos do AWS Connect por meio do Connect Console e de APIs públicas.

`AmazonConnect_FullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonConnect_FullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 20 de novembro de 2020, 19:54 UTC
- Hora da edição: 07 de março de 2023, 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnect_FullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "connect:*",
        "ds:CreateAlias",
        "ds:AuthorizeApplication",
        "ds:CreateIdentityPoolDirectory",
        "ds:DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:UnauthorizeApplication",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lex:GetBots",
        "lex:ListBots",
        "lex:ListBotAliases",
        "logs:CreateLogGroup",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "lambda:ListFunctions",
        "ds:CheckAlias",
        "profile:ListAccountIntegrations",
        "profile:GetDomain",
        "profile:ListDomains",
        "profile:GetProfileObjectType",
        "profile:ListProfileObjectTypeTemplates"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "profile:AddProfileKey",
        "profile:CreateDomain",
        "profile:CreateProfile",
```

```
        "profile:DeleteDomain",
        "profile:DeleteIntegration",
        "profile:DeleteProfile",
        "profile:DeleteProfileKey",
        "profile:DeleteProfileObject",
        "profile:DeleteProfileObjectType",
        "profile:GetIntegration",
        "profile:GetMatches",
        "profile:GetProfileObjectType",
        "profile:ListIntegrations",
        "profile:ListProfileObjects",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "profile:MergeProfiles",
        "profile:PutIntegration",
        "profile:PutProfileObject",
        "profile:PutProfileObjectType",
        "profile:SearchProfiles",
        "profile:TagResource",
        "profile:UntagResource",
        "profile:UpdateDomain",
        "profile:UpdateProfile"
      ],
      "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::amazon-connect-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "arn:aws:servicequotas:*:*:connect/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "connect.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:DeleteServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/profile.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "profile.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonConnectCampaignsServiceLinkedRolePolicy

Descrição: política de perfil vinculado ao serviço do Amazon Connect Campaigns

`AmazonConnectCampaignsServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 23 de setembro de 2021, 20:54 UTC
- Horário editado: 18 de junho de 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConnectCampaignAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect-campaigns:ListCampaigns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConnectCampaignsMetricsAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:GetMetricDataV2"
```

```
      ],
      "Resource" : "arn:aws:connect-campaigns:*:*:campaign/*"
    },
    {
      "Sid" : "ConnectAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:BatchPutContact",
        "connect:StopContact",
        "connect:DescribeContactFlow",
        "connect:SendOutboundEmail",
        "connect:SendOutboundWebNotification"
      ],
      "Resource" : "arn:aws:connect:*:*:instance/*"
    },
    {
      "Sid" : "ConnectChatAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:SendOutboundChatMessage"
      ],
      "Resource" : [
        "arn:aws:connect:*:*:instance/*",
        "arn:aws:connect:*:*:phone-number/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSocialMessagingSendMessageOperations",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:SendWhatsAppMessage"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:phone-number-id/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "AllowSocialMessagingTemplateOperations",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:GetWhatsAppMessageTemplate"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:waba/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSMSVoiceOperationsForConnect",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:SendTextMessage"
      ],
      "Resource" : "arn:aws:sms-voice:*:*:phone-number/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EventBridgeListRuleAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EventBridgeManagedResourceAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:DeleteRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ConnectCampaignsRule*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "connect-campaigns.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTargetsByRuleAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ConnectCampaignsRule*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowWisdomForConnectCampaignsEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:GetMessageTemplate",
        "wisdom:RenderMessageTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectCampaignsEnabled" : "True"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonConnectReadOnlyAccess

Descrição: Concede permissão para visualizar as instâncias do Amazon Connect em seu Conta da AWS.

`AmazonConnectReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonConnectReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de outubro de 2018, 21:00 UTC
- Hora da edição: 19 de junho de 2024, 15:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectReadOnly",
```

```
      "Effect" : "Allow",
      "Action" : [
        "connect:Get*",
        "connect:Describe*",
        "connect:List*",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyConnectEmergencyAccess",
      "Effect" : "Deny",
      "Action" : "connect:AdminGetEmergencyAccessToken",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonConnectServiceLinkedRolePolicy

Descrição: permite que o Amazon Connect crie e gerencie AWS recursos em seu nome.

`AmazonConnectServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Hora da criação: 07 de setembro de 2018, 0:21 UTC
- Horário editado: 02 de outubro de 2026, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

Versão da política

Versão da política: v56 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect_*"
    },
    {
      "Sid" : "AllowS3ObjectForConnectBucket",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-connect-*/*"
      ]
    },
    {
      "Sid" : "AllowGetBucketMetadataForConnectBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-connect-*"
      ]
    },
    {
      "Sid" : "AllowConnectLogGroupAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/connect/*:*"
      ]
    },
    {
      "Sid" : "AllowListLexBotAccess",
      "Effect" : "Allow",
      "Action" : [
        "lex:ListBots",
        "lex:ListBotAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCustomerProfilesForConnectDomain",
```

```
      "Effect" : "Allow",
      "Action" : "profile:*",
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*",
        "arn:aws:profile:*:*:/domains/amazon-connect-*",
        "arn:aws:profile:*:*:/templates*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowCustomerProfilesListOperations",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListRecommenderRecipes",
        "profile:ListAccountIntegrations",
        "profile:ListDomains"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DenyCustomerProfilesForConnectDomain",
      "Effect" : "Deny",
      "Action" : [
        "profile:CreateDomain",
        "profile:UpdateDomain",
        "profile:DeleteDomain",
        "profile:CreateEventStream",
        "profile:DeleteEventStream",
        "profile:DeleteWorkflow",
        "profile:DeleteProfileKey",
        "profile:UntagResource",
        "profile:TagResource",
        "profile:CreateIntegrationWorkflow"
      ],
      "Resource" : "arn:aws:profile:*:*:domains/*"
```

```
    },
    {
      "Sid" : "AllowAppIntegrationsForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "app-integrations:GetDataIntegration",
        "app-integrations:ListDataIntegrationAssociations",
        "app-integrations:CreateDataIntegrationSchedule",
        "app-integrations:StartDataIntegrationExecution",
        "app-integrations:ListDataIntegrationExecutions",
        "app-integrations:GetDataIntegrationExecution",
        "app-integrations:ListDataIntegrationSchedules",
        "app-integrations:UpdateDataIntegrationSchedule",
        "app-integrations:GetDataIntegrationSchedule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowWisdomForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "DenyWisdomForConnectEnabledTaggedResources",
      "Effect" : "Deny",
      "Action" : [
        "wisdom:DeleteAssistant",
        "wisdom:DeleteKnowledgeBase"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowListOperationForWisdom",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:ListAssistants",
        "wisdom:ListKnowledgeBases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSListRetirableGrants",
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    },
    {
      "Sid" : "AllowSMSVoiceOperationsForConnect",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:SendTextMessage",
        "sms-voice:DescribePhoneNumbers"
      ],
      "Resource" : "arn:aws:sms-voice:*:*:phone-number/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowCognitoForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:ListUserPoolClients"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowChimeSDKVoiceConnectorGetOperationForConnect",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetVoiceConnector"
      ],
      "Resource" : "arn:aws:chime:*:*:vc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowChimeSDKVoiceConnectorListOperationForConnect",
      "Effect" : "Allow",
      "Action" : [
        "chime:ListVoiceConnectors"
      ],
      "Resource" : "arn:aws:chime:*:*:vc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "SESPermissionsForManagingReceiptRules",
      "Effect" : "Allow",
      "Action" : [
        "ses:DescribeReceiptRule",
        "ses:UpdateReceiptRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SESPermissionForManagingConnectProvidedSESIdentity",
      "Effect" : "Allow",
      "Action" : [
        "ses:DeleteEmailIdentity"
      ],
      "Resource" : "arn:aws:ses:*:*:identity/*.email.connect.aws*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SESConfigurationSetPermissionsForSendingEmail",
      "Effect" : "Allow",
      "Action" : [
        "ses:SendRawEmail"
      ],
      "Resource" : "arn:aws:ses:*:*:configuration-set/configuration-set-for-connect-DO-
NOT-DELETE",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "PassRoleToSESForReceiptRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonConnectEmailSESAccessRole"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ses.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSocialMessagingOperations",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:SendWhatsAppMessage",
        "social-messaging:PostWhatsAppMessageMedia",
        "social-messaging:GetWhatsAppMessageMedia",
        "social-messaging:GetLinkedWhatsAppBusinessAccountPhoneNumber",
        "social-messaging:SendWhatsAppCallEvent"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:phone-number-id/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowRetrievalOfWabas",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:ListLinkedWhatsAppBusinessAccounts"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "AllowRetrievalOfWhatsAppTemplates",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:GetWhatsAppMessageTemplate",
        "social-messaging:ListWhatsAppMessageTemplates"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:waba/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowMobileTargetingOperationsForConnect",
      "Effect" : "Allow",
      "Action" : "mobiletargeting:SendMessages",
      "Resource" : "arn:aws:mobiletargeting:*:*:apps/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPollyActions",
      "Effect" : "Allow",
      "Action" : [
        "polly:ListLexicons",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonConnectSynchronizationServiceRolePolicy

Descrição: permite que o Amazon Connect sincronize AWS recursos entre regiões em seu nome.

`AmazonConnectSynchronizationServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 27 de outubro de 2023, 22:38 UTC
- Horário editado: 21 de novembro de 2025, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:Create*",
        "connect:BatchCreate*",
        "connect:Update*",
        "connect:BatchUpdate*",
        "connect:Delete*",
        "connect:BatchDelete*",
        "connect:Describe*",
        "connect:BatchDescribe*",
        "connect:List*",
        "connect:Search*",
        "connect:Associate*",
        "connect:Disassociate*",
        "connect:Get*",
        "connect:BatchGet*",
        "connect:Import*",
        "connect:TagResource",
        "connect:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DisallowedConnectActions",
      "Effect" : "Deny",
      "Action" : [
        "connect:Start*",
        "connect:Stop*",
        "connect:Resume*",
        "connect:Suspend*",
        "connect:*Contact",
        "connect:SearchContacts",
        "connect:*ContactAttributes*",
        "connect:*RealtimeContact*",
        "connect:*AnalyticsData*",
        "connect:*MetricData*",
        "connect:*UserData*",
        "connect:*ContactEvaluation",
        "connect:*AttachedFile*",
        "connect:UpdateContactSchedule",
        "connect:UpdateContactRoutingData",
        "connect:ListContactReferences",
```

```
        "connect:CreateParticipant",
        "connect:CreatePersistentContactAssociation",
        "connect:CreateInstance",
        "connect:DeleteInstance",
        "connect:ListInstances",
        "connect:ReplicateInstance",
        "connect:GetFederationToken",
        "connect:ClaimPhoneNumber",
        "connect:ImportPhoneNumber",
        "connect:ReleasePhoneNumber",
        "connect:SearchAvailablePhoneNumbers",
        "connect:CreateTrafficDistributionGroup",
        "connect:DeleteTrafficDistributionGroup",
        "connect:GetTrafficDistribution",
        "connect:UpdateTrafficDistribution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonConnectVoiceIDFullAccess

Descrição: fornece acesso total ao Amazon Connect Voice ID

`AmazonConnectVoiceIDFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonConnectVoiceIDFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de setembro de 2021, 19:04 UTC
- Hora da edição: 26 de setembro de 2021, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "voiceid:*",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDataZoneBedrockModelConsumptionPolicy

Descrição: Fornece permissões para consumir modelos do Amazon Bedrock, incluindo invocar o perfil de inferência do aplicativo Amazon Bedrock criado para um domínio específico da Amazon. DataZone

`AmazonDataZoneBedrockModelConsumptionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDataZoneBedrockModelConsumptionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 12 de novembro de 2024, 22:15 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneBedrockModelConsumptionPolicy`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InvokeDomainInferenceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
```

```
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "ListFoundationModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockCreateSessionWithTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateSession",
        "bedrock:TagResource"
      ],
      "Resource" : "arn:aws:bedrock:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/AmazonDataZoneUser" : "${datazone:userId}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${datazone:userId}",
          "aws:RequestTag/AmazonDataZoneDomain" : "${datazone:domainId}",
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}"
        },
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneUser" : "",
          "aws:ResourceTag/AmazonDataZoneUser" : "",
          "aws:RequestTag/AmazonDataZoneDomain" : "",
          "aws:ResourceTag/AmazonDataZoneDomain" : ""
        },
        "ForAllValues:StringLike" : {
```

```
          "aws:TagKeys" : "AmazonDataZone*"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockSessionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetSession",
        "bedrock:UpdateSession",
        "bedrock:DeleteSession",
        "bedrock:EndSession",
        "bedrock:CreateInvocation",
        "bedrock:ListInvocations",
        "bedrock:PutInvocationStep",
        "bedrock:GetInvocationStep",
        "bedrock:ListInvocationSteps",
        "bedrock:ListTagsForResource"
      ],
      "Resource" : "arn:aws:bedrock:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${datazone:userId}",
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}"
        },
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "",
          "aws:ResourceTag/AmazonDataZoneDomain" : ""
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockListSessionsPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListSessions",
      "Resource" : "*"
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDataZoneBedrockModelManagementPolicy

Descrição: fornece permissões para gerenciar o acesso ao modelo do Amazon Bedrock, incluindo criar, marcar e excluir perfis de inferência de aplicações.

`AmazonDataZoneBedrockModelManagementPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDataZoneBedrockModelManagementPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 12 de novembro de 2024, 22:14 UTC
- Horário editado: 12 de novembro de 2024, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneBedrockModelManagementPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageApplicationInferenceProfile",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile",
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteApplicationInferenceProfile",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "CreateApplicationInferenceProfileUsingFoundationModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "CreateApplicationInferenceProfileUsingBedrockModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDataZoneDomainExecutionRolePolicy

Descrição: Política padrão para a função DataZone de DomainExecutionRole serviço da Amazon. Essa função é usada pela Amazon DataZone para catalogar, descobrir, governar, compartilhar e analisar dados no DataZone domínio da Amazon.

`AmazonDataZoneDomainExecutionRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDataZoneDomainExecutionRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 27 de setembro de 2023, 21:55 UTC
- Horário editado: 26 de fevereiro de 2026, 00:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy`

Versão da política

Versão da política: v13 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DomainExecutionRoleStatement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateRule",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetFilter",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataProduct",
        "datazone:DeleteDataSource",
        "datazone:DeleteDomainUnit",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteRule",
```

```
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:DeleteTimeSeriesDataPoints",
        "datazone:GetAsset",
        "datazone:GetAssetFilter",
        "datazone:GetAssetType",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetLineageNode",
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
        "datazone:GetProject",
        "datazone:GetRule",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetFilters",
        "datazone:ListAssetRevisions",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
```

```
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListMetadataGenerationRuns",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListRules",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:ListWarehouseMetadata",
        "datazone:QueryGraph",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RemoveEntityOwner",
        "datazone:RemovePolicyGrant",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
```

```
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareStatement",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShareAssociations",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDataZoneEnvironmentRolePermissionsBoundary

Descrição: a Amazon DataZone cria funções do IAM para ambientes para realizar ações de análise de dados e usa essa política ao criar essas funções para definir o limite de suas permissões.

`AmazonDataZoneEnvironmentRolePermissionsBoundary` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDataZoneEnvironmentRolePermissionsBoundary` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de setembro de 2023, 23:38 UTC

- Hora da edição: 17 de novembro de 2023, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateGlueConnection",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      }
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : [
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
```

```
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
```

```
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SameAccountKmsOperations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KmsOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:Verify",
        "kms:Sign"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AnalyticsOperations",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*",
        "sqlworkbench:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QueryOperations",
      "Effect" : "Allow",
```

```
      "Action" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:Describe*",
```

```
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:SearchTables",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListGroups",
```

```
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeMetricFilters",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "secretsmanager:ListSecrets",
        "tag:GetResources"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "QueryOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryResultsStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsManagerOperationsWithTagKeys",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AmazonDataZoneDomain" : "*",
          "aws:ResourceTag/AmazonDataZoneProject" : "*"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        }
      }
    },
    {
      "Sid" : "DataZoneS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
```

```
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/datazone/*"
      ]
    },
    {
      "Sid" : "DataZoneS3BucketLocation",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListDataZoneS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "*/datazone/*",
            "datazone/*"
          ]
        }
      }
    },
    {
      "Sid" : "NotDeniedOperations",
      "Effect" : "Deny",
      "NotAction" : [
        "datazone:*",
        "sqlworkbench:*",
        "athena:BatchGetNamedQuery",
```

```
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteTags",
```

```
        "ec2:Describe*",
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
```

```
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:List*",
        "iam:PassRole",
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ListKeys",
        "kms:Verify",
        "kms:Sign",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
```

```
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:TagResource",
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDataZoneFullAccess

Descrição: Fornece acesso total à Amazon DataZone por meio do Console de gerenciamento da AWS , bem como acesso limitado aos serviços relacionados que são exigidos por ela.

`AmazonDataZoneFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDataZoneFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 22 de setembro de 2023, 20:06 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullAccess`

Versão da política

Versão da política: v13 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "secretsmanager:ListSecrets",
        "iam:ListUsers",
        "glue:GetDatabases",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codewhisperer:ListProfiles",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListFoundationModels",
        "bedrock:ListTagsForResource",
        "aoss:ListSecurityPolicies"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "BucketReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "CreateBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "ConfigureBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketCORS",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RamCreateResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RamResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RamResourceReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations",
        "ram:ListResourceSharePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RamAssociateResourceSharePermissionStatement",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:PermissionArn" : [
```

```
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMGetPolicyStatement",
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
      "Sid" : "DataZoneTagOnCreateDomainProjectTags",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "DataZoneTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "CreateSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "ConnectionStatement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "TagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:TagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "for-use-with-all-datazone-projects"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "UntagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UntagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "for-use-with-all-datazone-projects"
        }
      }
    },
    {
```

```
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
        "aoss:CreateSecurityPolicy"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "genai-studio-*"
        }
      }
    },
    {
      "Sid" : "GetFoundationModelStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "GetInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*",
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ]
    },
    {
      "Sid" : "ApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "TagApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDataZoneFullUserAccess

Descrição: Fornece acesso total à Amazon DataZone, mas não permite o gerenciamento de domínios, usuários ou contas associadas.

`AmazonDataZoneFullUserAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDataZoneFullUserAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 22 de setembro de 2023, 21:06 UTC
- Horário editado: 19 de novembro de 2024, 21:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneUserOperations",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
```

```
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateRule",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetFilter",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataProduct",
        "datazone:DeleteDataSource",
        "datazone:DeleteDomainUnit",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteRule",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
```

```
        "datazone:DeleteTimeSeriesDataPoints",
        "datazone:GetAsset",
        "datazone:GetAssetFilter",
        "datazone:GetAssetType",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetIamPortalLoginUrl",
        "datazone:GetLineageNode",
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
        "datazone:GetProject",
        "datazone:GetRule",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetFilters",
        "datazone:ListAssetRevisions",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
```

```
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListMetadataGenerationRuns",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListRules",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:ListWarehouseMetadata",
        "datazone:PostTimeSeriesDataPoints",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RemoveEntityOwner",
        "datazone:RemovePolicyGrant",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "RAMResourceShareOperations",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShareAssociations",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDataZoneGlueManageAccessRolePolicy

Descrição: A política concede permissões para permitir que a Amazon habilite DataZone a publicação e acesse concessões aos dados.

`AmazonDataZoneGlueManageAccessRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDataZoneGlueManageAccessRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 22 de setembro de 2023, 20:21 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy`

Versão da política

Versão da política: v18 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueTagDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringLikeIfExists" : {
          "aws:TagKeys" : "DataZoneDiscoverable_*"
        }
      }
    },
    {
      "Sid" : "GlueDataQuality",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListDataQualityResults",
        "glue:GetDataQualityResult"
      ],
      "Resource" : "arn:aws:glue:*:*:dataQualityRuleset/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "GlueCrawler",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnection",
      "Effect" : "Allow",
      "Action" : "glue:GetConnection",
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueTableDatabaseCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:GetDatabases",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:CreateCatalog",
        "glue:CreateDatabase",
        "glue:DeleteCatalog",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
```

```
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueGetTags",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTags",
        "glue:GetCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LakeformationResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:CreateDataCellsFilter",
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteDataCellsFilter",
        "lakeformation:DeleteLakeFormationOptIn",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
```

```
        "lakeformation:RevokePermissions",
        "lakeformation:UpdateDataCellsFilter",
        "glue:GetDatabase",
        "glue:GetTable",
        "organizations:DescribeOrganization",
        "ram:GetResourceShareInvitations",
        "ram:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LakeformationResourceFederatedSharing",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "lakeformation:GlueARN" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteResourcePolicy",
        "glue:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountLakeFormationResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceShareInvitation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*"
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DeleteResourceShare",
        "ram:DisassociateResourceShare",
        "ram:ListResourceSharePermissions",
```

```
        "ram:UpdateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetResourceSharesViaLakeFormation",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShares",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ram:PermissionArn" : "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "KMSDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/datazone:projectId" : "proj-all"
        }
      }
    },
    {
      "Sid" : "GetRoleForDataZone",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/AmazonSageMakerManageAccess*",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerManageAccess*"
      ]
    },
    {
      "Sid" : "PassRoleForDataLocationRegistration",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/AmazonSageMakerManageAccess*",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerManageAccess*",
        "arn:aws:iam::*:role/datazone_usr_role*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lakeformation.amazonaws.com",
```

```
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateCatalogEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateCatalogS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging"
      ],
      "Resource" : "arn:aws:s3:::redshift-staging-bucket*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDataZonePortalFullAccessPolicy

Descrição: Fornece acesso total às DataZone APIs da Amazon

`AmazonDataZonePortalFullAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDataZonePortalFullAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de março de 2023, 18:24 UTC
- Hora da edição: 26 de março de 2023, 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : "datazonecontrol:*",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDataZonePreviewConsoleFullAccess

Descrição: Fornece acesso total à versão prévia da Amazon DataZone por meio do Console de gerenciamento da AWS. Também fornece acesso seleto a outros serviços relacionados.

`AmazonDataZonePreviewConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDataZonePreviewConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de março de 2023, 15:16 UTC
- Hora da edição: 13 de julho de 2023, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "datazonecontrol:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "glue:GetConnections",
        "glue:GetDatabase",
        "redshift:DescribeClusters",
        "ec2:DescribeSubnets",
        "secretsmanager:ListSecrets",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/AmazonDataZone-*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneBootstrapServicePolicy-
AmazonDataZoneBootstrapRole",
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneServicePolicy-
AmazonDataZoneServiceRole"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZoneServiceRole*",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneServiceRole*",
        "arn:aws:iam::*:role/AmazonDataZoneBootstrapRole*",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneBootstrapRole",
        "arn:aws:iam::*:role/AmazonDataZoneDomainExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneDomainExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazonecontrol.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDataZoneProjectDeploymentPermissionsBoundary

Descrição: a Amazon DataZone cria funções do IAM que usa para implantar projetos de análise de dados. DataZone usa essa política ao criar essas funções para definir o limite de suas permissões.

`AmazonDataZoneProjectDeploymentPermissionsBoundary` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDataZoneProjectDeploymentPermissionsBoundary` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 21 de março de 2023, 2:54 UTC
- Hora da edição: 04 de abril de 2023, 2:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*datazone*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneProjectRolePermissionsBoundary"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateKey",
        "kms:TagResource",
        "athena:CreateWorkGroup",
        "athena:TagResource",
        "iam:TagRole",
        "iam:TagPolicy",
        "logs:CreateLogGroup",
        "logs:TagLogGroup",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "datazone:*"
        },
        "StringLike" : {
```

```
          "aws:ResourceTag/datazone:projectId" : "proj-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup",
        "kms:ScheduleKeyDeletion",
        "kms:DescribeKey",
        "kms:EnableKeyRotation",
        "kms:DisableKeyRotation",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:Decrypt",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/datazone:projectId" : "proj-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "datazone:projectId"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "s3:DeleteBucket"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:policy/datazone*",
        "arn:aws:s3:::datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetRolePolicy",
        "iam:CreatePolicy",
        "iam:ListPolicyVersions",
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:ListPermissions",
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabases",
        "glue:GetDatabase",
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:DeleteBucketPolicy",
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketAcl",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging",
        "s3:PutBucketLogging",
        "s3:GetObject*",
        "s3:GetBucket*",
        "s3:List*",
        "s3:GetEncryptionConfiguration",
        "s3:DeleteObject*",
        "s3:PutObject*",
        "s3:Abort*"
      ],
      "Resource" : "arn:aws:s3:::*datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:Get*",
        "athena:List*",
        "ec2:CreateSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup",
        "ec2:Describe*",
        "ec2:Get*",
        "ec2:List*",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogGroups",
        "logs:DeleteLogGroup",
```

```
        "logs:DeleteRetentionPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:PutKeyPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.logs",
            "com.amazonaws.*.s3",
            "com.amazonaws.*.glue",
            "com.amazonaws.*.athena"
          ]
        }
      }
    },
    {
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
```

```
        "cloudformation:GetTemplate",
        "cloudformation:DescribeChangeSet",
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:TagResource",
        "cloudformation:GetTemplateSummary"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "s3:GetObject*",
        "s3:GetBucket*",
        "s3:List*",
        "s3:GetEncryptionConfiguration",
        "s3:DeleteObject*",
        "s3:PutObject*",
        "s3:Abort*",
        "s3:DeleteBucket"
      ],
      "NotResource" : [
        "arn:aws:s3:::*datazone*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Effect" : "Deny",
      "NotAction" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:AddTagsToResource",
        "ssm:GetParameters",
        "ssm:GetParameter",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:DeleteBucketPolicy",
        "s3:CreateBucket",
        "s3:PutBucketAcl",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:DeleteBucket",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:CreatePolicy",
        "iam:ListPolicyVersions",
        "iam:DeletePolicy",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeChangeSet",
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:TagResource",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplateSummary",
        "athena:*",
        "kms:*",
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabases",
        "glue:GetDatabase",
        "lambda:*",
```

```
        "ec2:*",
        "logs:*",
        "servicecatalog:CreateApplication",
        "servicecatalog:DeleteApplication",
        "servicecatalog:GetApplication",
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy",
        "iam:UntagRole",
        "iam:PassRole",
        "iam:TagRole",
        "s3:GetBucket*",
        "s3:GetObject*",
        "s3:Abort*",
        "s3:GetEncryptionConfiguration",
        "s3:PutObject*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDataZoneProjectRolePermissionsBoundary

Descrição: a Amazon DataZone cria funções do IAM para projetos realizarem ações de análise de dados e usa essa política ao criar essas funções para definir o limite de suas permissões.

`AmazonDataZoneProjectRolePermissionsBoundary` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDataZoneProjectRolePermissionsBoundary` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 21 de março de 2023, 2:51 UTC
- Hora da edição: 21 de março de 2023, 2:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:List*",
        "s3:Get*",
        "s3:DeleteObjectVersion",
        "s3:RestoreObject",
        "s3:ReplicateObject",
```

```
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutObjectRetention",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:List*",
        "s3:Get*",
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "logs:*",
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGet*",
```

```
        "athena:List*",
        "athena:UpdateNotebook",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
        "athena:DeleteNamedQuery",
        "athena:Get*",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "lakeformation:GetDataAccess",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "ram:CreateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:AcceptResourceShareInvitation",
        "ram:Get*",
        "ram:List*",
        "redshift:DescribeClusters",
        "redshift:JoinGroup",
        "redshift:CreateClusterUser",
        "redshift:GetClusterCredentials",
        "redshift-data:*",
        "redshift:AuthorizeDataShare",
        "redshift:DescribeDataShares",
        "redshift:AssociateDataShareConsumer",
        "tag:GetResources",
        "iam:ListRoles",
```

```
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "glue:CreateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateDataQualityRuleset",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateWorkflow",
        "sqlworkbench:*",
        "datazone:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt",
```

```
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:GenerateDataKey",
        "glue:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/datazone:projectId" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGet*",
        "glue:SearchTables",
        "glue:List*",
        "glue:Get*",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:PutResourcePolicy",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
```

```
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:UpdatePartition",
        "glue:NotifyEvent",
        "glue:DeleteResourcePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "NotAction" : [
        "s3:List*",
        "s3:Get*",
        "s3:Describe*",
        "s3:DeleteObjectVersion",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutObjectRetention",
        "s3:DeleteObject",
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:GenerateDataKey",
        "ec2:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "logs:*",
        "athena:*",
        "glue:BatchGet*",
        "glue:Get*",
        "glue:SearchTables",
        "glue:List*",
        "glue:CreateDatabase",
```

```
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:PutResourcePolicy",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:UpdatePartition",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
```

```
        "glue:StartJobRun",
        "glue:CreateWorkflow",
        "glue:*DataQuality*",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "lakeformation:GetDataAccess",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "ram:*",
        "redshift:*",
        "redshift-data:*",
        "tag:GetResources",
        "iam:List*",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:PassRole",
        "sqlworkbench:*",
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDataZoneRedshiftGlueProvisioningPolicy

Descrição: DataZone A Amazon é um serviço de gerenciamento de dados que permite catalogar, descobrir, governar, compartilhar e analisar seus dados. Com a Amazon DataZone, você pode compartilhar e acessar seus dados em todas as contas e regiões suportadas. A Amazon DataZone simplifica sua experiência em todos AWS os serviços, incluindo, mas não se limitando a, Amazon Redshift, Amazon Athena, AWS Glue e AWS Lake Formation.

`AmazonDataZoneRedshiftGlueProvisioningPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDataZoneRedshiftGlueProvisioningPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 22 de setembro de 2023, 20:19 UTC
- Horário editado: 21 de agosto de 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZonePermissionsToCreateEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneEnvironmentRolePermissionsBoundary",
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ],
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToManageCreatedEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:GetRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneCFStackCreationForEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneCFStackManagementForEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
```

```
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:ListPermissions",
        "glue:CreateDatabase",
        "glue:GetDatabase",
        "athena:GetWorkGroup",
        "logs:DescribeLogGroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift:DescribeClusters",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentGlueDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteDatabase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentAthenaDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentAthenaResourceCreation",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateWorkGroup",
        "athena:TagResource",
        "iam:TagRole",
        "iam:TagPolicy",
        "logs:TagLogGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLogGroupCreation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLogGroupManagement",
      "Action" : [
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentIAMPolicyManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
```

```
        "iam:CreatePolicy",
        "iam:GetPolicy",
        "iam:ListPolicyVersions",
        "iam:DeletePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentS3ValidationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentKMSDecryptPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTagAmazonDataZoneEnvironmentGlueResources",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToGetAmazonDataZoneEnvironmentBlueprintTemplates",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "RedshiftDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ListSchemas",
        "redshift-data:ExecuteStatement"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "DescribeStatementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetSecretValuePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDataZoneRedshiftManageAccessRolePolicy

Descrição: Essa política concede à Amazon DataZone permissões para publicar dados do Amazon Redshift no catálogo. Ele também dá à Amazon DataZone permissões para conceder acesso ou revogar o acesso aos ativos publicados no catálogo do Amazon Redshift ou do Amazon Redshift Serverless.

`AmazonDataZoneRedshiftManageAccessRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDataZoneRedshiftManageAccessRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 22 de setembro de 2023, 20:15 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "redshiftDataScopeDownPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:ListTables",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift:*:*:cluster:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "listSecretsPermission",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "getWorkgroupPermission",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetWorkgroup",
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "createAndDeleteWorkgroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:DeleteWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "getNamespacePermission",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetNamespace",
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "createAndDeleteNamespacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:DeleteNamespace"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "redshiftDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "dataSharesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare",
        "redshift:DescribeDataShares"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:datashare:*/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "associateDataShareConsumerPermission",
      "Effect" : "Allow",
      "Action" : "redshift:AssociateDataShareConsumer",
      "Resource" : "arn:aws:redshift:*:*:datashare:*/datazone*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

Descrição: A AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary política é a lista de permissões permitidas em uma função de execução criada em um SageMaker ambiente provisionado pela Amazon. DataZone

`AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de abril de 2024, 23:01 UTC
- Horário editado: 17 de julho de 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`

Versão da política

Versão da política: v13 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
```

```
    },
    {
      "Sid" : "AllowSageMakerProfileManagement",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile",
        "sagemaker:UpdateUserProfile",
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:*/*"
    },
    {
      "Sid" : "AllowLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAddTagsForDomainResources",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:user-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : [
            "CreateApp",
            "CreateSpace",
            "CreateUserProfile"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStudioActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListApps",
        "sagemaker:ListDomains",
        "sagemaker:ListSpaces",
        "sagemaker:ListUserProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppActionsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAppActionsForSharedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Shared"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private",
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
```

```
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceActions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*",
        "datazone:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
```

```
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:StartImageScan",
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "groundtruthlabeling:*",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
```

```
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:UpdateLogDelivery",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-serverless:GetCredentials",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowRAMInvitation",
      "Effect" : "Allow",
      "Action" : "ram:AcceptResourceShareInvitation",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : "dzd*"
        }
      }
    },
    {
```

```
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker*",
        "arn:aws:ecr:*:*:repository/datazone*"
      ]
    },
    {
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:*sagemaker*",
        "arn:aws:codecommit:*:*:*SageMaker*",
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
      ]
```

```
    },
    {
      "Sid" : "AllowStepFunctionsActions",
      "Effect" : "Allow",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ]
    },
    {
      "Sid" : "AllowSecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::Sagemaker-DataZone*",
        "arn:aws:s3:::DataZone-Sagemaker*",
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::amazon-datazone*"
      ]
    },
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
      "Resource" : [
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::Sagemaker-DataZone*",
        "arn:aws:s3:::DataZone-Sagemaker*",
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::amazon-datazone*"
      ]
    },
    {
      "Sid" : "ReadSageMakerJumpstartArtifacts",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
```

```
        "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
      ],
```

```
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr_sagemaker_execution_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "bedrock.amazonaws.com",
            "states.amazonaws.com",
            "lakeformation.amazonaws.com",
            "events.amazonaws.com",
            "sagemaker.amazonaws.com",
            "forecast.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountKmsOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "KmsOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:RetireGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
```

```
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
```

```
      ]
    },
    {
      "Sid" : "AllowListTags",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:domain/*"
      ]
    },
    {
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:ListJobs",
        "glue:CreateSession",
        "glue:RunStatement",
        "glue:BatchCreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:BatchDeletePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:UpdateTable",
        "glue:DeleteTableVersion",
        "glue:DeleteTable",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
```

```
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchDeleteTable",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:UpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:GetDatabases",
        "glue:GetTables",
        "glue:GetTable",
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:ListSchemas",
        "glue:BatchGetJobs",
        "glue:GetConnection",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueActionsWithEnvironmentTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
```

```
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:ListSchemas",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:CreateWorkflow",
        "glue:*DataQuality*"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGlueDefaultAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGet*",
        "glue:Get*",
        "glue:SearchTables",
        "glue:List*",
        "glue:RunStatement"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default",
```

```
        "arn:aws:glue:*:*:connection/dz-sm-*",
        "arn:aws:glue:*:*:session/*"
      ]
    },
    {
      "Sid" : "AllowRedshiftClusterActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowCreateClusterUser",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateClusterUser"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*"
      ]
    },
    {
      "Sid" : "AllowCreateSecretActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneProject" : "false",
```

```
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "ForecastOperations",
      "Effect" : "Allow",
      "Action" : [
        "forecast:CreateExplainabilityExport",
        "forecast:CreateExplainability",
        "forecast:CreateForecastEndpoint",
        "forecast:CreateAutoPredictor",
        "forecast:CreateDatasetImportJob",
        "forecast:CreateDatasetGroup",
        "forecast:CreateDataset",
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast:CreatePredictorBacktestExportJob",
        "forecast:CreatePredictor",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeExplainability",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeForecastEndpoint",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeDataset",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:GetAccuracyMetrics",
        "forecast:InvokeForecastEndpoint",
        "forecast:GetRecentForecastContext",
        "forecast:DescribePredictor",
        "forecast:TagResource",
        "forecast:DeleteResourceTree"
      ],
      "Resource" : [
        "arn:aws:forecast:*:*:*Canvas*"
      ]
```

```
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEventBridgeRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeTagBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
```

```
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTagOperation",
      "Effect" : "Allow",
      "Action" : "events:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEMR",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSSOAction",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplicationAssignment",
        "sso:AssociateProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyNotAction",
      "Effect" : "Deny",
      "NotAction" : [
        "sagemaker:*",
        "sagemaker-geospatial:*",
        "sqlworkbench:*",
        "datazone:*",
        "forecast:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
```

```
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
```

```
        "athena:UpdatePreparedStatement",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:CreateRepository",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
```

```
        "ecr:PutImage",
        "ecr:StartImageScan",
        "ecr:TagResource",
        "ecr:UntagResource",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListClusters",
        "events:PutRule",
        "events:DescribeRule",
        "events:PutTargets",
        "events:TagResource",
        "events:ListTagsForResource",
        "fsx:DescribeFileSystems",
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:BatchGet*",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:Get*",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:CreateWorkflow",
```

```
        "glue:*DataQuality*",
        "glue:List*",
        "glue:CreateSession",
        "glue:RunStatement",
        "glue:BatchCreatePartition",
        "glue:CreateDatabase",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:BatchUpdatePartition",
        "glue:BatchDeletePartition",
        "glue:UpdateTable",
        "glue:DeleteTableVersion",
        "glue:DeleteTable",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchDeleteTable",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:UpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "groundtruthlabeling:*",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:RetireGrant",
        "lakeformation:GetDataAccess",
        "lambda:ListFunctions",
        "lambda:InvokeFunction",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
```

```
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:UpdateLogDelivery",
        "ram:AcceptResourceShareInvitation",
        "rds:DescribeDBInstances",
        "redshift:CreateClusterUser",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:DescribeClusters",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors",
        "s3:DeleteObjectVersion",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "secretsmanager:ListSecrets",
```

```
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:TagResource",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:ProvisionProduct",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish",
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine",
        "tag:GetResources",
        "sso:CreateApplicationAssignment",
        "sso:AssociateProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyUpdateNotebookInstanceLifecycleConfig",
      "Effect" : "Deny",
      "Action" : [
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDataZoneSageMakerManageAccessRolePolicy

Descrição: A AmazonDataZoneSageMakerManageAccessRolePolicy política concede à Amazon DataZone as permissões necessárias para conceder ao usuário acesso a vários recursos no SageMaker ambiente.

`AmazonDataZoneSageMakerManageAccessRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDataZoneSageMakerManageAccessRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de abril de 2024, 23:34 UTC
- Horário editado: 12 de fevereiro de 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerManageAccessRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:ListModelPackages",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:ListTags",
        "sagemaker:DescribeDomain",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:Search"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerTaggingPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:shared-with:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelPackageGroupPolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:DeleteModelPackageGroupPolicy"
```

```
      ],
      "Resource" : [
        "arn:*:sagemaker:*:*:model-package-group/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerRAMPermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerRAMResourcePolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:PutResourcePolicy",
        "sagemaker:GetResourcePolicy",
        "sagemaker:DeleteResourcePolicy"
      ],
      "Resource" : [
        "arn:*:sagemaker:*:*:feature-group/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerRAMTagResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : "arn:*:ram:*:*:resource-share/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerRAMDeleteResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ram:DeleteResourceShare"
      ],
      "Resource" : "arn:*:ram:*:*:resource-share/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerRAMCreateResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "sagemaker:*"
          ]
        },
        "Null" : {
          "aws:RequestTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerS3BucketPolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
```

```
    {
      "Sid" : "AmazonSageMakerS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetRepositoryPolicy",
        "ecr:SetRepositoryPolicy",
        "ecr:DeleteRepositoryPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerKMSReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AmazonSageMakerKMSGrantPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDataZoneSageMakerProvisioningRolePolicy

Descrição: A AmazonDataZoneSageMakerProvisioningRolePolicy política concede à Amazon DataZone as permissões necessárias para interoperar com a Amazon SageMaker.

`AmazonDataZoneSageMakerProvisioningRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDataZoneSageMakerProvisioningRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de abril de 2024, 23:32 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerProvisioningRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSageMakerStudio",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateDomain"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
```

```
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false",
          "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteSageMakerStudio",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteDomain"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentSageMakerDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "sagemaker.amazonaws.com"
          ],
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToCreateEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ],
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToManageEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToCreateSageMakerServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "sagemaker:ListDomains"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentKMSKeyValidation",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentGluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection",
        "glue:DeleteConnection",
        "glue:GetConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/dz-sm-athena-glue-connection-*",
        "arn:aws:glue:*:*:connection/dz-sm-redshift-cluster-connection-*",
        "arn:aws:glue:*:*:connection/dz-sm-redshift-serverless-connection-*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
```

```
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDetectiveFullAccess

Descrição: fornece acesso total ao serviço Amazon Detective e acesso limitado às dependências da interface do usuário do console

`AmazonDetectiveFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDetectiveFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário da criação: 30 de abril de 2020, 17:57 UTC
- Hora da edição: 17 de maio de 2023, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:*",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings"
      ],
      "Resource" : "arn:aws:guardduty:*:*:detector/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "securityHub:GetFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDetectiveInvestigatorAccess

Descrição: fornece acesso de investigador ao serviço Amazon Detective e acesso limitado às dependências da interface do usuário do console. Esta política concede permissão para entrar em Detective para fins de investigação e acesso de gravação limitado ao GuardDuty.

`AmazonDetectiveInvestigatorAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDetectiveInvestigatorAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de janeiro de 2023, 15:24 UTC
- Hora da edição: 27 de novembro de 2023, 3:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DetectivePermissions",
      "Effect" : "Allow",
      "Action" : [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDatasourcePackages",
        "detective:ListGraphs",
        "detective:ListHighDegreeEntities",
        "detective:ListInvitations",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "detective:SearchGraph",
        "detective:StartInvestigation",
        "detective:GetInvestigation",
        "detective:ListInvestigations",
        "detective:UpdateInvestigationState",
        "detective:ListIndicators",
        "detective:InvokeAssistant"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "GuardDutyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings",
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "securityHub:GetFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDetectiveMemberAccess

Descrição: fornece acesso de membro ao serviço Amazon Detective e acesso limitado às dependências da interface do usuário do console.

`AmazonDetectiveMemberAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDetectiveMemberAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de janeiro de 2023, 15:16 UTC
- Hora da edição: 17 de janeiro de 2023, 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDetectiveOrganizationsAccess

Descrição: fornece acesso às organizações para gerenciar o administrador delegado do Amazon Detective e acesso limitado às dependências da interface do usuário do console. Isso também concede permissão para criar uma função vinculada ao serviço para o Detective.

`AmazonDetectiveOrganizationsAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDetectiveOrganizationsAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 02 de março de 2023, 15:20 UTC
- Hora da edição: 02 de março de 2023, 15:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "detective.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "detective.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "detective.amazonaws.com",
            "guardduty.amazonaws.com",
            "macie.amazonaws.com",
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDetectiveServiceLinkedRolePolicy

Descrição: permite que o Amazon Detective faça chamadas de serviço em seu nome

`AmazonDetectiveServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 18 de novembro de 2021, 19:47 UTC
- Hora da edição: 18 de novembro de 2021, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDevOpsGuruConsoleFullAccess

Descrição: A política concede acesso total ao console do DevOps Guru.

`AmazonDevOpsGuruConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDevOpsGuruConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de dezembro de 2021, 18:43 UTC
- Hora da edição: 25 de agosto de 2022, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsListTopicsAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsTopicOperations",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
    },
    {
      "Sid" : "DevOpsGuruSlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "DevOpsGuruSlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PerformanceInsightsMetricsDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics",
        "pi:DescribeDimensionKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDevOpsGuruFullAccess

Descrição: Fornece acesso total ao Amazon DevOps Guru.

`AmazonDevOpsGuruFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDevOpsGuruFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2020, 16:38 UTC
- Hora da edição: 25 de agosto de 2022, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsListTopicsAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsTopicOperations",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Publish"
      ],
```

```
      "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
    },
    {
      "Sid" : "DevOpsGuruSlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DevOpsGuruSlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDevOpsGuruOrganizationsAccess

Descrição: Forneça acesso para habilitar e gerenciar o Amazon DevOps Guru dentro de uma organização.

`AmazonDevOpsGuruOrganizationsAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDevOpsGuruOrganizationsAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de novembro de 2021, 23:50 UTC
- Hora da edição: 15 de novembro de 2021, 23:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:SearchOrganizationInsights"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListRoots"
      ],
      "Resource" : "arn:aws:organizations::*:"
    },
    {
      "Sid" : "OrganizationsAdminDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "devops-guru.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDevOpsGuruReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon DevOps Guru Console.

`AmazonDevOpsGuruReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDevOpsGuruReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2020, 16:34 UTC
- Hora da edição: 25 de agosto de 2022, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:DescribeAccountHealth",
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
        "devops-guru:DescribeResourceCollectionHealth",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetCostEstimation",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListAnomaliesForInsight",
        "devops-guru:ListEvents",
        "devops-guru:ListInsights",
        "devops-guru:ListAnomalousLogGroups",
        "devops-guru:ListMonitoredResources",
        "devops-guru:ListNotificationChannels",
        "devops-guru:ListRecommendations",
        "devops-guru:SearchInsights",
        "devops-guru:StartCostEstimation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDevOpsGuruServiceRolePolicy

Descrição: É necessária uma função vinculada ao serviço para que DevOpsGuru a Amazon acesse seus recursos.

`AmazonDevOpsGuruServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 1º de dezembro de 2020, 10:24 UTC
- Hora da edição: 10 de janeiro de 2023, 14:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudtrail:LookupEvents",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:ListDashboards",
        "cloudwatch:GetDashboard",
        "cloudformation:GetTemplate",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListImports",
        "codedeploy:BatchGetDeployments",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:ListDeployments",
        "config:DescribeConfigurationRecorderStatus",
        "config:GetResourceConfigHistory",
        "events:ListRuleNamesByTarget",
        "xray:GetServiceGraph",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "pi:GetResourceMetrics",
        "tag:GetResources",
        "lambda:GetFunction",
        "lambda:GetFunctionConcurrency",
        "lambda:GetAccountSettings",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:ListAliases",
        "lambda:ListEventSourceMappings",
        "lambda:GetPolicy",
        "ec2:DescribeSubnets",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
```

```
        "sqs:GetQueueAttributes",
        "kinesis:DescribeStream",
        "kinesis:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeStream",
        "dynamodb:ListStreams",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeAccountAttributes",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "s3:GetBucketNotification",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketWebsite",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListStorageLensConfigurations",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListServiceQuotas"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutTargetsOnASpecificRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOps-Guru-managed-*"
    },
    {
```

```
      "Sid" : "AllowCreateOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAddTagsToOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Sid" : "AllowAccessOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-GuruInsightSsmOpsItemRelated" : "true"
        }
      }
    },
    {
      "Sid" : "AllowCreateManagedRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
    },
    {
      "Sid" : "AllowAccessManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
    },
```

```
    {
      "Sid" : "AllowOtherOperationsOnManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowTagBasedFilterLogEvents",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAPIGatewayGetIntegrations",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/??????????",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDMSCloudWatchLogsRole

Descrição: fornece acesso ao upload de registros de replicação do DMS para os logs do CloudWatch na conta do cliente.

`AmazonDMSCloudWatchLogsRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDMSCloudWatchLogsRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 07 de janeiro de 2016, 23:44 UTC
- Hora da edição: 23 de maio de 2023, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribeOnAllLogGroups",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeOfAllLogStreamsOnDmsTasksLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*"
      ]
    },
    {
      "Sid" : "AllowCreationOfDmsLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:"
      ]
    },
    {
      "Sid" : "AllowCreationOfDmsLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
      ]
    },
    {
      "Sid" : "AllowUploadOfLogEventsToDmsLogStream",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDMSRedshiftS3Role

Descrição: fornece acesso para gerenciar as configurações do S3 dos endpoints do Redshift para DMS.

`AmazonDMSRedshiftS3Role` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDMSRedshiftS3Role` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 20 de abril de 2016, 17:05 UTC
- Hora da edição: 08 de julho de 2019, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:DeleteBucket",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:GetBucketAcl",
        "s3:PutBucketVersioning",
        "s3:GetBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:DeleteBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::dms-*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDMSVPCManagementRole

Descrição: fornece acesso para gerenciar configurações de VPC para configurações AWS gerenciadas de clientes

`AmazonDMSVPCManagementRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDMSVPCManagementRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 18 de novembro de 2015, 16:33 UTC
- Hora da edição: 25 de julho de 2024, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDocDB-ElasticServiceRolePolicy

Descrição: Permite que DocumentDB-Elastic a Amazon gerencie AWS recursos em seu nome.

`AmazonDocDB-ElasticServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Hora da criação: 30 de novembro de 2022, 14:17 UTC
- Hora da edição: 30 de novembro de 2022, 14:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB-Elastic"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDocDBConsoleFullAccess

Descrição: fornece acesso total para gerenciar o Amazon DocumentDB compatível com MongoDB usando o Console de gerenciamento da AWS. Importante notar que essa política também proporciona acesso total para publicação em todos os tópicos SNS da conta, permissões para criar e modificar instâncias do Amazon EC2 e configurações de VPC, autorizações para visualizar e listar chaves no Amazon KMS, além de acesso completo ao Amazon RDS e ao Amazon Neptune.

`AmazonDocDBConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDocDBConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de janeiro de 2019, 20:37 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DocdbSids",
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
```

```
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic:DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource",
        "docdb-elastic:CopyClusterSnapshot",
        "docdb-elastic:StartCluster",
        "docdb-elastic:StopCluster",
        "docdb-elastic:GetPendingMaintenanceAction",
        "docdb-elastic:ListPendingMaintenanceActions",
        "docdb-elastic:ApplyPendingMaintenanceAction",
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DeleteGlobalCluster",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
```

```
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:ModifyGlobalCluster",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveFromGlobalCluster",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "DependencySids",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DocdbSLRSid",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DocdbElasticSLRSid",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDocDBElasticFullAccess

Descrição: Fornece acesso total aos clusters elásticos do Amazon DocumentDB e outras permissões necessárias para suas dependências, incluindo EC2, KMS e IAM. SecretsManager CloudWatch

`AmazonDocDBElasticFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDocDBElasticFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 05 de junho de 2023, 13:51 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DocdbElasticSid",
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic:DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource",
        "docdb-elastic:CopyClusterSnapshot",
        "docdb-elastic:StartCluster",
        "docdb-elastic:StopCluster",
        "docdb-elastic:GetPendingMaintenanceAction",
        "docdb-elastic:ListPendingMaintenanceActions",
        "docdb-elastic:ApplyPendingMaintenanceAction"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2Sid",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KMSSid",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
          ],
          "aws:ResourceTag/DocDBElasticFullAccess" : "*"
        }
      }
    },
    {
      "Sid" : "KMSGrantSid",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/DocDBElasticFullAccess" : "*",
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
```

```
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "SecretManagerSid",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:GetResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/DocDBElasticFullAccess" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudwatchSid",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SLRSid",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
```

```
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDocDBElasticReadOnlyAccess

Descrição: Fornece acesso somente para leitura à Amazon DocDB-Elastic e CloudWatch às métricas.

`AmazonDocDBElasticReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDocDBElasticReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de junho de 2023, 14:37 UTC
- Hora da edição: 21 de junho de 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:ListClusters",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDocDBFullAccess

Descrição: fornece acesso total ao Amazon DocumentDB compatível com MongoDB. É importante observar que esta política também proporciona acesso total para a publicação em todos os tópicos do SNS dentro da conta, além de acesso completo ao Amazon RDS e ao Amazon Neptune.

`AmazonDocDBFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDocDBFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de janeiro de 2019, 20:21 UTC
- Hora da edição: 09 de janeiro de 2019, 20:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
```

```
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
```

```
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDocDBReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon DocumentDB compatível com MongoDB. Observe que essa política também concede acesso aos atributos do Amazon RDS e do Amazon Neptune.

`AmazonDocDBReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDocDBReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de janeiro de 2019, 20:30 UTC
- Hora da edição: 09 de janeiro de 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "kms:ListAliases",
        "kms:ListKeyPolicies"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

Gerenciamento de RSVPC do Amazon

Descrição: fornece acesso para gerenciar configurações de VPC para configurações de clientes gerenciadas pela Amazon

`AmazonDRSVPCManagement` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDRSVPCManagement` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 02 de setembro de 2015, 0:09 UTC
- Hora da edição: 02 de setembro de 2015, 0:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDRSVPCManagement`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDynamoDBFullAccess

Descrição: Fornece acesso total ao Amazon DynamoDB por meio do. Console de gerenciamento da AWS

`AmazonDynamoDBFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDynamoDBFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 29 de janeiro de 2021, 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess`

Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "dynamodb:*",
        "dax:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:GetMetricData",
        "datapipeline:ActivatePipeline",
```

```
        "datapipeline:CreatePipeline",
        "datapipeline:DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:PutPipelineDefinition",
        "datapipeline:QueryObjects",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes",
        "lambda:CreateFunction",
        "lambda:ListFunctions",
        "lambda:ListEventSourceMappings",
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping",
        "lambda:GetFunctionConfiguration",
        "lambda:DeleteFunction",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupQuery",
        "resource-groups:DeleteGroup",
        "resource-groups:CreateGroup",
        "tag:GetResources",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
```

```
    {
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com",
            "application-autoscaling.amazonaws.com.cn",
            "dax.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.dynamodb.amazonaws.com",
            "dax.amazonaws.com",
            "dynamodb.application-autoscaling.amazonaws.com",
            "contributorinsights.dynamodb.amazonaws.com",
            "kinesisreplication.dynamodb.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDynamoDBFullAccess_v2

Descrição: fornece acesso total ao Amazon DynamoDB

`AmazonDynamoDBFullAccess_v2` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDynamoDBFullAccess_v2` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 22 de maio de 2025, 14:52 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess_v2`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "DDBAndDAXFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:*",
        "dax:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSIntegration",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaIntegration",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DaxSNSIntegration",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingIntegration",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "dynamodb"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchMonitoring",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListKinesisResources",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ListEC2ResourcesForDaxClusterCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchInsightsRules",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Sid" : "ServiceRoleCreation",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.dynamodb.amazonaws.com",
            "dax.amazonaws.com",
            "dynamodb.application-autoscaling.amazonaws.com",
            "contributorinsights.dynamodb.amazonaws.com",
            "kinesisreplication.dynamodb.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamIntegration",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDynamoDBFullAccesswithDataPipeline

Descrição: esta política será descontinuada. Consulte a documentação para obter orientação: https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html. Fornece acesso total ao Amazon DynamoDB, incluindo o Export/Import uso do AWS Data Pipeline por meio do. Console de gerenciamento da AWS

`AmazonDynamoDBFullAccesswithDataPipeline` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDynamoDBFullAccesswithDataPipeline` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 12 de novembro de 2015, 2:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "dynamodb:*",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsole"
    },
    {
      "Action" : [
        "lambda:*",
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsoleTriggers"
    },
    {
      "Action" : [
```

```
        "datapipeline:*",
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsoleImportExport"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRolePolicy",
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Sid" : "IAMEDPRoles"
    },
    {
      "Action" : [
        "ec2:CreateTags",
        "ec2:DescribeInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "elasticmapreduce:*",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "EMR"
    },
    {
      "Action" : [
        "s3:DeleteObject",
        "s3:Get*",
        "s3:List*",
        "s3:Put*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
```

```
      "Sid" : "S3"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonDynamoDBReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon DynamoDB por meio do. Console de gerenciamento da AWS

`AmazonDynamoDBReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonDynamoDBReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 18 de novembro de 2024, 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess`

Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralReadOnlyAccess",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb:GetAbacStatus",
        "dynamodb:GetItem",
        "dynamodb:GetResourcePolicy",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dax:Describe*",
        "dax:List*",
        "dax:GetItem",
        "dax:BatchGetItem",
        "dax:Query",
        "dax:Scan",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
```

```
        "kms:ListAliases",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "lambda:ListFunctions",
        "lambda:ListEventSourceMappings",
        "lambda:GetFunctionConfiguration",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupQuery",
        "tag:GetResources",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CCIAccess",
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEBSCSIDriverEKSClusterScopedPolicy

Descrição: política do IAM que permite que a conta do serviço de driver da CSI faça chamadas para serviços relacionados, como o EC2, em seu nome. Essa política restringe o driver CSI do Amazon EBS ao gerenciamento apenas de volumes e snapshots do EBS que pertençam a um cluster EKS específico. Ela exige a tag de recurso ebs.csi.aws. com/cluster-name para corresponder à tag

eks-cluster-name no principal do IAM, impedindo o acesso entre clusters quando vários clusters compartilham o mesmo. Conta da AWS As operações de anexação e desconexão em instâncias são restritas a instâncias marcadas com a tag eks:cluster-name (definida automaticamente pelo EKS em grupos de nós gerenciados) ou ebs.csi.aws. com/clustertag -name (para instâncias marcadas manualmente).

`AmazonEBSCSIDriverEKSClusterScopedPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEBSCSIDriverEKSClusterScopedPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 16 de abril de 2026, 17:27 UTC
- Horário editado: 28 de maio de 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEBSCSIDriverEKSClusterScopedPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyDescribeOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
```

```
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateAndCopyVolumesWithClusterTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "CopyClusterVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/vol-*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsWithClusterTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsFromClusterVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "ManageClusterVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "CreateVolumesFromAndEnableFSROnClusterSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "AttachDetachVolumesToClusterInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/eks:cluster-name" : "${aws:PrincipalTag/eks-cluster-name}"
        }
      }
    },
    {
      "Sid" : "AttachDetachVolumesToEKSStandardTaggedInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks-cluster-
name}"
        }
      }
    },
    {
      "Sid" : "AttachDetachVolumesToManuallyTaggedInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "DeleteAndLockClusterSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        }
      }
    },
    {
      "Sid" : "TagResourcesOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot",
            "CopyVolumes"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "ModifyTagsOnClusterVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster-name" : "${aws:PrincipalTag/eks-
cluster-name}"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringNotEquals" : {
          "aws:TagKeys" : [
            "ebs.csi.aws.com/cluster",
            "ebs.csi.aws.com/cluster-name",
            "kubernetes.io/created-for/pvc/name"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEBSCSIDriverPolicy

Descrição: política do IAM que permite que a conta do serviço de driver da CSI faça chamadas para serviços relacionados, como o EC2, em seu nome.

`AmazonEBSCSIDriverPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEBSCSIDriverPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 04 de abril de 2022, 17:24 UTC
- Horário editado: 13 de maio de 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy`

Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/vol-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot",
            "CopyVolumes"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/CSIVolumeName" : "*"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/kubernetes.io/created-for/pvc/name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
```

```
        "StringLike" : {
          "aws:RequestTag/CSIVolumeSnapshotName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeSnapshotName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEBSCSIDriverPolicyV2

Descrição: Política de IAM que permite que a conta de serviço de motorista CSI do EBS faça chamadas para serviços relacionados, como o EC2, em seu nome. Isso limita o driver CSI do Amazon EBS ao gerenciamento apenas de volumes e snapshots do EBS marcados com a chave ebs.csi.aws. com/cluster definido como verdadeiro. Os volumes provisionados pelo plug-in de volume Kubernetes in-tree (CSI-migrated volumes) também são suportados pelo kubernetes. io/created- tag de recurso for/pvc /name.

`AmazonEBSCSIDriverPolicyV2` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEBSCSIDriverPolicyV2` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 16 de abril de 2026, 17:27 UTC
- Horário editado: 16 de abril de 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEBSCSIDriverPolicyV2`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyDescribeOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateAndCopyVolumesWithManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Sid" : "CopyManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:volume/vol-*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Sid" : "CopyCSIMigratedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/vol-*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/kubernetes.io/created-for/pvc/name" : "*"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsWithManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsFromManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "ManageManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Sid" : "ManageCSIMigratedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/kubernetes.io/created-for/pvc/name" : "*"
        }
      }
    },
    {
      "Sid" : "CreateVolumesFromAndEnableFSROnManagedSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Sid" : "AttachDetachVolumesToAnyInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DeleteAndLockManagedSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Sid" : "TagResourcesOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot",
            "CopyVolumes"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "ModifyTagsOnManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringNotEquals" : {
          "aws:TagKeys" : [
            "ebs.csi.aws.com/cluster",
            "ebs.csi.aws.com/cluster-name",
            "kubernetes.io/created-for/pvc/name"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEC2ContainerRegistryFullAccess

Descrição: fornece acesso administrativo a recursos do Amazon ECR

`AmazonEC2ContainerRegistryFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2ContainerRegistryFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 21 de dezembro de 2015, 17:06 UTC
- Hora da edição: 05 de dezembro de 2020, 0:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:*",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.ecr.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEC2ContainerRegistryPowerUser

Descrição: fornece acesso total aos repositórios do Amazon EC2 Container Registry, mas não permite a exclusão do repositório nem alterações nas políticas.

`AmazonEC2ContainerRegistryPowerUser` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2ContainerRegistryPowerUser` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 21 de dezembro de 2015, 17:05 UTC
- Hora da edição: 10 de dezembro de 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEC2ContainerRegistryPullOnly

Descrição: fornece acesso para extrair imagens dos repositórios do Amazon EC2 Container Registry.

`AmazonEC2ContainerRegistryPullOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2ContainerRegistryPullOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 4 de outubro de 2024, 16:58 UTC
- Hora da edição: 4 de outubro de 2024, 16:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPullOnly`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
```

```
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchImportUpstreamImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEC2ContainerRegistryReadOnly

Descrição: fornece acesso somente leitura aos repositórios do Amazon EC2 Container Registry.

`AmazonEC2ContainerRegistryReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2ContainerRegistryReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 21 de dezembro de 2015, 17:04 UTC
- Hora da edição 10 de dezembro de 2019, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEC2ContainerServiceAutoscaleRole

Descrição: política para habilitar o ajuste de escala automático de tarefas para o Amazon EC2 Container Service

`AmazonEC2ContainerServiceAutoscaleRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2ContainerServiceAutoscaleRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 12 de maio de 2016, 23:25 UTC
- Hora da edição: 05 de fevereiro de 2018, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEC2ContainerServiceEventsRole

Descrição: Política para habilitar CloudWatch eventos para o EC2 Container Service

`AmazonEC2ContainerServiceEventsRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2ContainerServiceEventsRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço

- Hora da criação: 30 de maio de 2017, 16:51 UTC
- Hora da edição: 06 de março de 2023, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:RunTask"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ecs-tasks.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "ecs:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RunTask"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEC2ContainerServiceforEC2Role

Descrição: política padrão para o perfil do Amazon EC2 para o Amazon EC2 Container Service.

`AmazonEC2ContainerServiceforEC2Role` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2ContainerServiceforEC2Role` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 19 de março de 2015, 18:45 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags",
        "ecs:CreateCluster",
        "ecs:DeregisterContainerInstance",
        "ecs:DiscoverPollEndpoint",
        "ecs:Poll",
        "ecs:RegisterContainerInstance",
        "ecs:StartTelemetrySession",
        "ecs:UpdateContainerInstancesState",
        "ecs:Submit*",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterContainerInstance"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*/*",
        "arn:aws:ecs:*:*:container-instance/*/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEC2ContainerServiceRole

Descrição: política padrão para o perfil de serviço do Amazon ECS.

`AmazonEC2ContainerServiceRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2ContainerServiceRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 09 de abril de 2015, 16:14 UTC

- Hora da edição: 11 de agosto de 2016, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEC2FullAccess

Descrição: Fornece acesso total ao Amazon EC2 por meio do Console de gerenciamento da AWS.

`AmazonEC2FullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2FullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 27 de novembro de 2018, 2:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "ec2:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "ec2scheduled.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "transitgateway.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEC2ImageReferencesAccessPolicy

Descrição: fornece acesso somente para leitura para verificar todos os tipos de recursos compatíveis em busca de dados relevantes durante o uso. DescribeImageReferences

`AmazonEC2ImageReferencesAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2ImageReferencesAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 26 de agosto de 2025, 19:19 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ImageReferencesAccessPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:DescribeImageReferences",
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ssm:DescribeParameters",
        "ssm:GetParameters",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:GetContainerRecipe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ec2-images.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEC2ReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon EC2 por meio do Console de gerenciamento da AWS.

`AmazonEC2ReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2ReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 12 de fevereiro de 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEC2RoleforAWSCodeDeploy

Descrição: fornece ao EC2 acesso ao bucket do S3 para baixar a revisão. Essa função é necessária para o CodeDeploy agente nas instâncias do EC2.

`AmazonEC2RoleforAWSCodeDeploy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2RoleforAWSCodeDeploy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 19 de maio de 2015, 18:10 UTC
- Hora da edição: 20 de março de 2017, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEC2RoleforAWSCodeDeployLimited

Descrição: fornece ao EC2 acesso limitado ao bucket do S3 para baixar a revisão. Essa função é necessária para o CodeDeploy agente nas instâncias do EC2.

`AmazonEC2RoleforAWSCodeDeployLimited` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2RoleforAWSCodeDeployLimited` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 24 de agosto de 2020, 17:55 UTC
- Hora da edição: 20 de janeiro de 2022, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEC2RoleforDataPipelineRole

Descrição: política padrão para o perfil do Amazon EC2 para o perfil de serviço do Data Pipeline.

`AmazonEC2RoleforDataPipelineRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2RoleforDataPipelineRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 22 de fevereiro de 2016, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "datapipeline:*",
        "dynamodb:*",
        "ec2:Describe*",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListInstance*",
        "elasticmapreduce:ModifyInstanceGroups",
        "rds:Describe*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "s3:*",
        "sdb:*",
        "sns:*",
        "sqs:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

Função do Amazon EC2 para SSM

Descrição: esta política será descontinuada em breve. Use a AmazonSSMManagedInstanceCore política para ativar a funcionalidade principal do serviço do AWS Systems Manager em instâncias do EC2. Para obter mais informações, consulte https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html

`AmazonEC2RoleforSSM` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2RoleforSSM` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 29 de maio de 2015, 17:48 UTC
- Hora da edição: 24 de janeiro de 2019, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
```

```
        "ssm:GetManifest",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeInstanceStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetEncryptionConfiguration",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEC2RolePolicyForLaunchWizard

Descrição: Política gerenciada para a função de LaunchWizard serviço da Amazon para EC2

`AmazonEC2RolePolicyForLaunchWizard` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2RolePolicyForLaunchWizard` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 13 de novembro de 2019, 8:05 UTC
- Horário editado: 18 de agosto de 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardResourceGroupID" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceRoute"
      ],
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeRegions",
        "ec2:DescribeVolumes",
        "ec2:DescribeRouteTables",
        "ec2:ModifyInstanceAttribute",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricData",
```

```
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LaunchWizardResourceGroupID",
            "LaunchWizardApplicationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/LaunchWizardResourceGroupID" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVolume"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
```

```
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardResourceGroupID" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:GetBucketLocation",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*",
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:Create*",
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "cloudformation:DescribeStackResources",
        "cloudformation:SignalResource",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "LaunchWizardResourceGroupID"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:PutItem",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "dynamodb:Scan",
        "s3:ListBucket",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteTable",
        "dynamodb:CreateTable",
        "s3:GetObject",
        "dynamodb:DescribeTable",
        "s3:GetBucketLocation",
        "dynamodb:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:dynamodb:*:*:table/LaunchWizard*",
        "arn:aws:sqs:*:*:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSSAP-InstallBackint",
        "arn:aws:ssm:*:*:document/AWSSAP-InstallBackintForAWSBackup"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:ListTagsForResource",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEC2SpotFleetAutoscaleRole

Descrição: política para habilitar o ajuste de escala automático para a frota spot do Amazon EC2

`AmazonEC2SpotFleetAutoscaleRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2SpotFleetAutoscaleRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço

- Hora da criação: 19 de agosto de 2016, 18:27 UTC
- Hora da edição: 18 de fevereiro de 2019, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ec2.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEC2SpotFleetTaggingRole

Descrição: permite que o EC2 Spot Fleet solicite, encerre e marque instâncias spot em seu nome.

`AmazonEC2SpotFleetTaggingRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEC2SpotFleetTaggingRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 29 de junho de 2017, 18:19 UTC
- Hora da edição: 23 de abril de 2020, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      },
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
```

```
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:*/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

Amazon ECS_ FullAccess

Descrição: Fornece acesso administrativo aos recursos do Amazon ECS e habilita os recursos do ECS por meio do acesso a outros recursos de AWS serviço, incluindo VPCs, grupos de Auto Scaling e pilhas. CloudFormation

`AmazonECS_FullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonECS_FullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 07 de novembro de 2017, 21:36 UTC
- Horário editado: 02 de setembro de 2026, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECS_FullAccess`

Versão da política

Versão da política: v22 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSIntegrationsManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:ListMeshes",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:Describe*",
        "autoscaling:UpdateAutoScalingGroup",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
```

```
        "cloudformation:DescribeStack*",
        "cloudformation:UpdateStack",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "codedeploy:BatchGetApplicationRevisions",
        "codedeploy:BatchGetApplications",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ContinueDeployment",
        "codedeploy:CreateApplication",
        "codedeploy:CreateDeployment",
        "codedeploy:CreateDeploymentGroup",
        "codedeploy:GetApplication",
        "codedeploy:GetApplicationRevision",
        "codedeploy:GetDeployment",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:GetDeploymentTarget",
        "codedeploy:ListApplicationRevisions",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentConfigs",
        "codedeploy:ListDeploymentGroups",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "codedeploy:RegisterApplicationRevision",
        "codedeploy:StopDeployment",
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CancelSpotFleetRequests",
        "ec2:CreateInternetGateway",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:Describe*",
        "ec2:DetachInternetGateway",
```

```
        "ec2:DisassociateRouteTable",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RequestSpotFleet",
        "ec2:RunInstances",
        "ecs:*",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget",
        "events:ListTargetsByRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "fsx:DescribeFileSystems",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRoles",
        "lambda:ListFunctions",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:FilterLogEvents",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "servicediscovery:CreatePrivateDnsNamespace",
        "servicediscovery:CreateService",
        "servicediscovery:DeleteService",
        "servicediscovery:GetNamespace",
```

```
        "servicediscovery:GetOperation",
        "servicediscovery:GetService",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:UpdateService",
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/aws/service/ecs*"
    },
    {
      "Sid" : "ManagedCloudformationResourcesCleanupPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteInternetGateway",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "EC2ContainerService-*"
        }
      }
    },
    {
      "Sid" : "TasksPassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
```

```
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ecs-tasks.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InfrastructurePassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsInfrastructureRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InstancePassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsInstanceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "AutoScalingPassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsAutoscaleRole*"
      ],
```

```
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com",
            "application-autoscaling.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "ServiceLinkedRoleCreationPolicy",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "ecs.amazonaws.com",
            "autoscaling.amazonaws.com",
            "ecs.application-autoscaling.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ELBTaggingPolicy",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateTargetGroup",
            "CreateRule",
            "CreateListener",
            "CreateLoadBalancer"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonECSComputeServiceRolePolicy

Descrição: política para permitir que o Amazon ECS Compute gerencie suas instâncias do EC2 e recursos relacionados como parte das instâncias gerenciadas do ECS.

`AmazonECSComputeServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 24 de março de 2025, 17:37 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSComputeServiceRolePolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyPermissionsForInstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeFleets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForInstanceEventWindows",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceEventWindows"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ReadOnlyPermissionsForLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteManagedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "TerminateManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonECSInfrastructureRoleforExpressGatewayServices

Descrição: Essas permissões permitem que o Amazon ECS provisione e gerencie automaticamente os componentes de infraestrutura necessários para o Express Gateway Services, incluindo balanceamento de carga, grupos de segurança, certificados SSL e configurações de escalabilidade automática.

`AmazonECSInfrastructureRoleforExpressGatewayServices` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonECSInfrastructureRoleforExpressGatewayServices` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 12 de novembro de 2025, 20:34 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRoleforExpressGatewayServices`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ServiceLinkedRoleCreateOperations",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ecs.application-autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ELBOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:ModifyRule",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteListener"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateELBResources",
```

```
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:AddTags",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer",
            "CreateListener",
            "CreateRule",
            "CreateTargetGroup"
          ]
        }
      }
    },
    {
      "Sid" : "BlanketAllowCreateSecurityGroupsInVPCs",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "CreateSecurityGroupResourcesWithTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ModifySecurityGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateEC2Resources",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "AuthorizeSecurityGroupIngress",
            "AuthorizeSecurityGroupEgress"
          ]
        }
      }
    },
    {
      "Sid" : "CertificateOperations",
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate",
        "acm:AddTagsToCertificate",
```

```
        "acm:DeleteCertificate",
        "acm:DescribeCertificate"
      ],
      "Resource" : [
        "arn:aws:acm:*:*:certificate/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingCreateOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:TagResource",
        "application-autoscaling:DeregisterScalableTarget"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingPolicyOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DeleteScalingPolicy"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "ecs"
        }
      }
```

```
    },
    {
      "Sid" : "ApplicationAutoscalingReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ]
    },
    {
      "Sid" : "CloudWatchAlarmCreateOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CloudWatchAlarmOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "ELBReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VPCReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsCreateOperations",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonECSInfrastructureRoleForGatewayHostSharedALB

Descrição: Política padrão para a função de infraestrutura do Amazon ECS para o Amazon ECS Service Gateway Services.

`AmazonECSInfrastructureRoleForGatewayHostSharedALB` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonECSInfrastructureRoleForGatewayHostSharedALB` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 25 de setembro de 2026, 21:17 UTC
- Horário editado: 25 de setembro de 2026, 21:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRoleForGatewayHostSharedALB`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ServiceLinkedRoleCreateOperations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticloadbalancing.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ELBOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:ModifyRule",
        "elasticloadbalancing:SetRulePriorities",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:SetSecurityGroups"
      ],
```

```
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateELBResources",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:AddTags",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer",
            "CreateListener",
            "CreateRule",
            "CreateTargetGroup"
          ]
        }
      }
    },
    {
      "Sid" : "BlanketAllowCreateSecurityGroupsInVPCs",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "CreateSecurityGroupResourcesWithTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
```

```
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ModifySecurityGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateEC2Resources",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
```

```
            "CreateSecurityGroup",
            "AuthorizeSecurityGroupIngress",
            "AuthorizeSecurityGroupEgress"
          ]
        }
      }
    },
    {
      "Sid" : "CertificateOperations",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:DeleteCertificate"
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CertificateCreateOperations",
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate"
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CertificateReadOperations",
      "Effect" : "Allow",
      "Action" : "acm:DescribeCertificate",
      "Resource" : "arn:aws:acm:*:*:certificate/*"
    },
    {
      "Sid" : "WAFAssociationOnALBs",
      "Effect" : "Allow",
      "Action" : [
```

```
        "wafv2:AssociateWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : "arn:aws:wafv2:*:*:regional/webacl/*/*"
    },
    {
      "Sid" : "ELBSetWebACLOnALBs",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateWebACLAssociation",
        "elasticloadbalancing:DeleteWebACLAssociation",
        "elasticloadbalancing:SetWebACL"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "WAFReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:wafv2:*:*:regional/webacl/*/*"
    },
    {
      "Sid" : "ELBGetWebACLOnALBs",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:GetLoadBalancerWebACL",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "ELBReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VPCReadOperations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonECSInfrastructureRolePolicyForLoadBalancers

Descrição: fornece acesso a outros recursos de AWS serviço necessários para gerenciar balanceadores de carga associados às cargas de trabalho do ECS em seu nome.

`AmazonECSInfrastructureRolePolicyForLoadBalancers` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonECSInfrastructureRolePolicyForLoadBalancers` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 17 de julho de 2025, 16:37 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForLoadBalancers`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ELBReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
    },
    {
      "Sid" : "ALBModifyListeners",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyListener",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*"
```

```
      ]
    },
    {
      "Sid" : "NLBModifyListeners",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyListener",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/net/*/*/*"
      ]
    },
    {
      "Sid" : "ALBModifyRules",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyRule",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonECSInfrastructureRolePolicyForManagedInstances

Descrição: fornece acesso ao ECS para criar e gerenciar recursos gerenciados pelo EC2

`AmazonECSInfrastructureRolePolicyForManagedInstances` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonECSInfrastructureRolePolicyForManagedInstances` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 26 de setembro de 2025, 18:04 UTC
- Horário editado: 15 de setembro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForManagedInstances`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateLaunchTemplateForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CreateLaunchTemplateVersionsForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ProvisionEC2InstancesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CreateFleetForSupportingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Sid" : "CreateFleetForECSManagedLaunchTemplates",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesForECSManagedLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonECSManaged" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "RunInstancesForSupportingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    },
    {
      "Sid" : "TagOnCreateEC2ResourcesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet",
            "CreateLaunchTemplate",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "PassInstanceRoleForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/ecsInstanceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.*"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRoleForEC2Spot",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot"
      ]
    },
    {
      "Sid" : "DescribeEC2ResourcesManagedByECS",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeCapacityReservations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListResourceGroupResources",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "tag:GetResources"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerS

Descrição: Fornece acesso administrativo à Autoridade de Certificação Privada, ao Gerenciador de AWS Segredos e a outros itens Serviços da AWS necessários para gerenciar os recursos TLS do ECS Service Connect em seu nome.

`AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 19 de janeiro de 2024, 20:08 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagOnCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
```

```
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RotateTLSCertificateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:UpdateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecretVersionStage"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "ecs-sc",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DescribeTLSCertificateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthority",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
```

```
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthorityForIssuingEndEntityCertificate",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true",
          "acm-pca:TemplateArn" : "arn:aws:acm-pca:::template/EndEntityCertificate/V1"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonECSInfrastructureRolePolicyForVolumes

Descrição: Fornece acesso a outros recursos AWS de serviço necessários para gerenciar volumes associados às cargas de trabalho do ECS em seu nome.

`AmazonECSInfrastructureRolePolicyForVolumes` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonECSInfrastructureRolePolicyForVolumes` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 10 de janeiro de 2024, 22:56 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "CreateEBSManagedVolumeFromSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Sid" : "TagOnCreateVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVolume",
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeVolumesForLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstancesForAttachingVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageEBSVolumeLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManageVolumeAttachmentsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DeleteEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:ResourceTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonECSInfrastructureRolePolicyForVpcLattice

Descrição: fornece acesso a outros recursos de AWS serviço necessários para gerenciar o recurso VPC Lattice em cargas de trabalho do ECS em seu nome.

`AmazonECSInfrastructureRolePolicyForVpcLattice` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonECSInfrastructureRolePolicyForVpcLattice` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 15 de novembro de 2024, 20:02 UTC
- Horário editado: 29 de setembro de 2026, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForVpcLattice`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManagedVpcLatticeTargetRegistration",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:RegisterTargets",
        "vpc-lattice:DeregisterTargets"
```

```
      ],
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
    },
    {
      "Sid" : "DescribeVpcLatticeTargetGroup",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:GetTargetGroup",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
    },
    {
      "Sid" : "ListVpcLatticeTargets",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:ListTargets",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
    },
    {
      "Sid" : "GetRule",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:GetRule",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:service/*/listener/*/rule/*"
      ]
    },
    {
      "Sid" : "UpdateRule",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:UpdateRule",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:service/*/listener/*/rule/*"
      ]
    },
    {
      "Sid" : "UpdateListener",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:UpdateListener",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:service/*/listener/*"
      ]
```

```
    },
    {
      "Sid" : "DescribeEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonECSInstanceRolePolicyForManagedInstances

Descrição: política padrão para a função de instância do Amazon ECS para as instâncias gerenciadas pelo Amazon ECS.

`AmazonECSInstanceRolePolicyForManagedInstances` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonECSInstanceRolePolicyForManagedInstances` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 26 de setembro de 2025, 23:49 UTC

- Horário editado: 02 de julho de 2026, 02:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInstanceRolePolicyForManagedInstances`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSAgentDiscoverPollEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DiscoverPollEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECSAgentRegisterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterContainerInstance"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/*"
    },
    {
      "Sid" : "ECSAgentPollPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:Poll"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:container-instance/*",
```

```
        "arn:aws:ecs:*:*:task-set/*"
      ]
    },
    {
      "Sid" : "ECSAgentTelemetryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:StartTelemetrySession",
        "ecs:PutSystemLogEvents"
      ],
      "Resource" : "arn:aws:ecs:*:*:container-instance/*"
    },
    {
      "Sid" : "ECSAgentStateChangePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:SubmitAttachmentStateChanges",
        "ecs:SubmitTaskStateChange"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonECSServiceRolePolicy

Descrição: política para permitir que o Amazon ECS gerencie seu cluster.

`AmazonECSServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 14 de outubro de 2017, 1:18 UTC
- Horário editado: 22 de abril de 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

Versão da política

Versão da política: v24 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSTaskManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:AssociateTrunkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:Describe*",
        "ec2:DetachNetworkInterface",
        "ec2:DisassociateTrunkInterface",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
```

```
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:Get*",
        "route53:List*",
        "route53:UpdateHealthCheck",
        "servicediscovery:DeregisterInstance",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:UpdateInstanceCustomHealthStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingManagement",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:SetInstanceProtection",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:PutLifecycleHook",
        "autoscaling:DeleteLifecycleHook",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:RecordLifecycleActionHeartbeat",
        "autoscaling:TerminateInstanceInAutoScalingGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "autoscaling:ResourceTag/AmazonECSManaged" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "AutoScalingPlanManagement",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling-plans:CreateScalingPlan",
        "autoscaling-plans:DeleteScalingPlan",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:DescribeScalingPlanResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ecs-managed-*"
    },
    {
      "Sid" : "EventBridgeRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CWAlarmManagement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
```

```
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ECSTagging",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "CWLogGroupManagement",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*"
    },
    {
      "Sid" : "CWLogStreamManagement",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*:log-stream:*"
    },
    {
      "Sid" : "ExecuteCommandSessionManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExecuteCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
```

```
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*",
        "arn:aws:ssm:*:*:document/AmazonECS-ExecuteInteractiveCommand"
      ]
    },
    {
      "Sid" : "OpenDataChannel",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudMapResourceCreation",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:CreateHttpNamespace",
        "servicediscovery:CreateService"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonECSManaged"
          ]
        }
      }
    },
    {
      "Sid" : "CloudMapResourceTagging",
      "Effect" : "Allow",
      "Action" : "servicediscovery:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:RequestTag/AmazonECSManaged" : "*"
        }
      }
    },
    {
      "Sid" : "CloudMapResourceDeletion",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DeleteService"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CloudMapResourceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudMapResourceAttributeManagement",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:UpdateServiceAttributes"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForInstanceEventWindows",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceEventWindows"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonECSTaskExecutionRolePolicy

Descrição: Fornece acesso a outros recursos AWS de serviço necessários para executar tarefas do Amazon ECS

`AmazonECSTaskExecutionRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonECSTaskExecutionRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 16 de novembro de 2017, 18:48 UTC
- Hora da edição: 16 de novembro de 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEFSCSIDriverPolicy

Descrição: fornece acesso de gerenciamento aos recursos do EFS e acesso de leitura ao EC2

`AmazonEFSCSIDriverPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEFSCSIDriverPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço

- Hora da criação: 25 de julho de 2023, 20:10 UTC
- Hora da edição: 25 de julho de 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateAccessPoint",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateAccessPoint"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
```

```
        }
      }
    },
    {
      "Sid" : "AllowTagNewAccessPoints",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticfilesystem:CreateAction" : "CreateAccessPoint"
        },
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
        }
      }
    },
    {
      "Sid" : "AllowDeleteAccessPoint",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:DeleteAccessPoint",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/efs.csi.aws.com/cluster" : "false"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKS_CNI_Policy

Descrição: esta política fornece ao plug-in CNI do Amazon VPC (amazon-vpc-cni-k8s) as permissões necessárias para modificar a configuração do endereço IP nos nós de processamento do EKS. Esse conjunto de permissões permite que o CNI liste, descreva e modifique o Elastic Network Interfaces em seu nome. Mais informações sobre o plug-in AWS VPC CNI estão disponíveis aqui: https://github.com/aws/amazon-vpc-cni-k8s

`AmazonEKS_CNI_Policy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEKS_CNI_Policy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de maio de 2018, 21:07 UTC
- Horário editado: 04 de março de 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSCNIPolicy",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:AssignPrivateIpAddresses",
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEKSCNIPolicyENITag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSBlockStoragePolicy

Descrição: política vinculada à função de cluster do EKS que concede permissões para gerenciar os recursos de armazenamento em blocos do cluster.

`AmazonEKSBlockStoragePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEKSBlockStoragePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 30 de outubro de 2024, 20:18 UTC
- Horário editado: 30 de outubro de 2024, 20:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSBlockStoragePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:ModifyVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "CSIVolumeName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "kubernetes.io/created-for/*",
            "Name",
            "KubernetesCluster"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "CSIVolumeSnapshotName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "Name"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSBlockStoragePolicyV2

Descrição: política vinculada à função de cluster do EKS que concede permissões para gerenciar os recursos de armazenamento em blocos do cluster.

`AmazonEKSBlockStoragePolicyV2` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEKSBlockStoragePolicyV2` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 11 de maio de 2026, 16:27 UTC
- Horário editado: 11 de maio de 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSBlockStoragePolicyV2`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:ModifyVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "CSIVolumeName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "kubernetes.io/created-for/*",
            "Name",
            "KubernetesCluster"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "CSIVolumeSnapshotName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "Name"
```

```
            ]
          }
        }
      }
    ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSClusterPolicy

Descrição: esta política fornece ao Kubernetes as permissões necessárias para gerenciar recursos em seu nome. O Kubernetes exige Ec2:CreateTags permissões para colocar informações de identificação nos recursos do EC2, incluindo, mas não se limitando a, instâncias, grupos de segurança e interfaces de rede elásticas.

`AmazonEKSClusterPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEKSClusterPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de maio de 2018, 21:06 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSClusterPolicy`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSClusterPolicy",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:UpdateAutoScalingGroup",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateRoute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteRoute",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DetachVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyVolume",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstanceTopology",
        "elasticloadbalancing:AddTags",
```

```
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:AttachLoadBalancerToSubnets",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateLoadBalancerPolicy",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancerListeners",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DetachLoadBalancerFromSubnets",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEKSClusterPolicySLRCreate",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AmazonEKSClusterPolicyENIDelete",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/eks:eni:owner" : "amazon-vpc-cni"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSComputePolicy

Descrição: política vinculada à função de cluster do EKS que concede permissões para gerenciar os recursos de computação em cluster.

`AmazonEKSComputePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEKSComputePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 01 de novembro de 2024, 21:46 UTC
- Horário editado: 18 de maio de 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSComputePolicy`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-node-class-name" : "*",
          "aws:RequestTag/eks:kubernetes-node-pool-name" : "*"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "eks:kubernetes-node-class-name",
            "eks:kubernetes-node-pool-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:AddRoleToInstanceProfile",
      "Resource" : "arn:aws:iam::*:instance-profile/eks*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DescribeCapacityReservations",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSConnectorServiceRolePolicy

Descrição: Essa política permite que o Amazon EKS gerencie AWS recursos para o conector EKS

`AmazonEKSConnectorServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 04 de setembro de 2021, 20:31 UTC
- Horário editado: 15 de outubro de 2025, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSConnectorServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessSSMService",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateActivation",
        "ssm:DescribeInstanceInformation",
        "ssm:DeleteActivation"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConnectorAgentStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:ssm:*::document/AmazonEKS-ExecuteNonInteractiveCommand"
      ]
    },
    {
      "Sid" : "ConnectorAgentDeregister",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeregisterManagedInstance"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "PassAnyRoleToSsm",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PutManagedEventRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : "aws.ssm"
        }
      }
    },
    {
      "Sid" : "PutManagedEventTarget",
      "Effect" : "Allow",
      "Action" : "events:PutTargets",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OpenDataChannel",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSDashboardConsoleReadOnly

Descrição: fornece acesso somente leitura à visualização do painel no console do Amazon EKS. O painel agrega informações sobre vários clusters e recursos relacionados usando AWS Organizações.

`AmazonEKSDashboardConsoleReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEKSDashboardConsoleReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 19 de junho de 2025, 17:22 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSDashboardConsoleReadOnly`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSDashboardReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListDashboardData",
        "eks:ListDashboardResources",
        "eks:DescribeClusterVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonOrganizationsReadOnly",
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonOrganizationsDelegatedAdmin",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "eks.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSDashboardServiceRolePolicy

Descrição: essa política permite que o painel do Amazon EKS acesse e exiba informações de toda a organização. A política permite que o serviço EKS Dashboard colete informações sobre a estrutura e as contas de sua AWS organização.

`AmazonEKSDashboardServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 08 de maio de 2025, 19:07 UTC
- Horário editado: 08 de maio de 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSDashboardServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOrganizationsReadActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization",
```

```
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSFargatePodExecutionRolePolicy

Descrição: Fornece acesso a outros recursos AWS de serviço necessários para executar pods do Amazon EKS no AWS Fargate

`AmazonEKSFargatePodExecutionRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEKSFargatePodExecutionRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 22 de novembro de 2019, 4:34 UTC
- Hora da edição: 22 de novembro de 2019, 4:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSForFargateServiceRolePolicy

Descrição: esta política concede permissões necessárias ao Amazon EKS para executar tarefas do Fargate

`AmazonEKSForFargateServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 22 de novembro de 2019, 4:36 UTC
- Hora da edição 22 de novembro de 2019, 4:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSForFargateServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSLoadBalancingPolicy

Descrição: política vinculada à função de cluster do EKS que concede permissões para gerenciar os recursos de balanceador de carga do cluster.

`AmazonEKSLoadBalancingPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEKSLoadBalancingPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 30 de outubro de 2024, 20:18 UTC
- Horário editado: 20 de agosto de 2026, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLoadBalancingPolicy`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateRule",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "ingress.eks.amazonaws.com/stack",
            "ingress.eks.amazonaws.com/resource",
            "service.eks.amazonaws.com/stack",
            "service.eks.amazonaws.com/resource",
            "gateway.eks.amazonaws.com.alb/stack",
            "gateway.eks.amazonaws.com.alb/resource",
            "gateway.eks.amazonaws.com.nlb/stack",
            "gateway.eks.amazonaws.com.nlb/resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group-rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "eks-cluster-sg*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer",
            "CreateTargetGroup",
            "CreateListener",
            "CreateRule"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "AuthorizeSecurityGroupIngress"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:SetIpAddressType",
        "elasticloadbalancing:SetSecurityGroups",
        "elasticloadbalancing:SetSubnets",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:ModifyListenerAttributes",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:ModifyRule",
        "elasticloadbalancing:ModifyIpPools",
        "elasticloadbalancing:ModifyCapacityReservation",
        "elasticloadbalancing:DescribeLoadBalancers"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:AssociateWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:CreateProtection",
        "shield:DeleteProtection"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:TagResource"
      ],
      "Resource" : "arn:aws:shield::*:protection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "ingress.eks.amazonaws.com/stack",
            "ingress.eks.amazonaws.com/resource",
            "service.eks.amazonaws.com/stack",
```

```
            "service.eks.amazonaws.com/resource",
            "gateway.eks.amazonaws.com.alb/stack",
            "gateway.eks.amazonaws.com.alb/resource",
            "gateway.eks.amazonaws.com.nlb/stack",
            "gateway.eks.amazonaws.com.nlb/resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPoolClient",
        "acm:ListCertificates",
        "acm:DescribeCertificate",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListWebACLs",
        "elasticloadbalancing:SetWebAcl",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:SetRulePriorities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeIpamPools"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSLocalOutpostClusterPolicy

Descrição: esta política fornece permissões para que as instâncias do ambiente de gerenciamento do cluster local do EKS executadas em sua conta gerenciem recursos em seu nome.

`AmazonEKSLocalOutpostClusterPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEKSLocalOutpostClusterPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 24 de agosto de 2022, 21:56 UTC
- Hora da edição: 24 de outubro de 2024, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeAvailabilityZones",
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:DescribeInstanceProperties",
        "ssm:DescribeDocumentParameters",
        "ssm:ListInstanceAssociations",
        "ssm:RegisterManagedInstance",
        "ssm:UpdateInstanceInformation",
```

```
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:PutComplianceItems",
        "ssm:PutInventory",
        "ecr-public:GetAuthorizationToken",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/eks/*",
        "arn:aws:ecr:*:*:repository/bottlerocket-admin",
        "arn:aws:ecr:*:*:repository/bottlerocket-control-eks",
        "arn:aws:ecr:*:*:repository/diagnostics-collector-eks",
        "arn:aws:ecr:*:*:repository/kubelet-config-updater"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:*:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSLocalOutpostServiceRolePolicy

Descrição: permite que o Amazon EKS Local ligue para AWS os serviços em seu nome.

`AmazonEKSLocalOutpostServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 23 de agosto de 2022, 21:53 UTC
- Horário editado: 26 de junho de 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribePlacementGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "CreateSecurityGroup",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "secretsmanager:DeleteSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:DescribeSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-local-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/eks-local:controlplane-name" : "*"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ssm:*::document/AmazonEKS-ControlPlaneInstanceProxy"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ResumeSession",
        "ssm:TerminateSession"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSMCPReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao serviço Amazon EKS MCP. Essa política concede permissões para usar somente ferramentas de leitura no serviço EKS MCP destinadas à observabilidade, solução de problemas, recuperação de informações de recursos do EKS e obtenção de sugestões. EKS-optimized

`AmazonEKSMCPReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEKSMCPReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 20 de novembro de 2025, 17:19 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSMCPReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:ListClusters",
        "eks:DescribeNodegroup",
        "eks:ListNodegroups",
```

```
        "eks:DescribeAddon",
        "eks:ListAddons",
        "eks:DescribeAccessEntry",
        "eks:ListAccessEntries",
        "eks:DescribeInsight",
        "eks:ListInsights",
        "eks:AccessKubernetesApi"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks-mcp:InvokeMcp",
        "eks-mcp:CallReadOnlyTool"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSNetworkingPolicy

Descrição: política vinculada à função de cluster do EKS que concede permissões para gerenciar os recursos de rede do cluster.

`AmazonEKSNetworkingPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEKSNetworkingPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Tempo de criação: 28 de outubro de 2024, 22:34 UTC
- Horário editado: 21 de agosto de 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSNetworkingPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-cni-node-name" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "eks:kubernetes-cni-node-name",
            "sgp.eks.amazonaws.com/instance-id",
            "sgp.eks.amazonaws.com/trunk-eni-id",
            "sgp.eks.amazonaws.com/vlan-id",
            "sgp.eks.amazonaws.com/managed",
```

```
            "sgp.eks.amazonaws.com/policy-ref"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:ModifyNetworkInterfaceAttribute",
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateTrunkInterface",
        "ec2:DisassociateTrunkInterface"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSServicePolicy

Descrição: esta política permite que o Amazon Elastic Container Service para Kubernetes crie e gerencie os atributos necessários para operar clusters do EKS.

`AmazonEKSServicePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEKSServicePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de maio de 2018, 21:08 UTC
- Hora da edição: 14 de outubro de 2024, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSServicePolicy`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "iam:ListAttachedRolePolicies",
        "eks:UpdateClusterVersion",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : "eks-cluster-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "route53:AssociateVPCWithHostedZone",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/eks.amazonaws.com/
AWSServiceRoleForAmazonEKS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "eks.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSServiceRolePolicy

Descrição: Uma Service-Linked função necessária para que o Amazon EKS chame AWS serviços em seu nome.

`AmazonEKSServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Hora da criação: 21 de fevereiro de 2020, 20:10 UTC
- Horário editado: 01 de outubro de 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy`

Versão da política

Versão da política: v28 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceStatus",
```

```
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkAcls",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "eks:DescribeCluster",
        "ec2:DescribeIpamPools",
        "ec2:DescribeTrunkInterfaceAssociations",
        "elasticloadbalancing:DescribeListenerAttributes",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DescribeTrustStores",
        "elasticloadbalancing:DescribeCapacityReservation",
        "iam:ListAttachedRolePolicies",
        "pricing:GetProducts",
        "shield:GetSubscriptionState",
        "shield:DescribeProtection",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/Name" : "eks-cluster-sg*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
```

```
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : "eks-cluster-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "route53:AssociateVPCWithHostedZone",
      "Resource" : "arn:aws:route53:::hostedzone/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "AWS/EKS"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateCertificateAuthority",
        "eks:DeleteCertificateAuthority",
```

```
        "eks:ActivateCertificateAuthority"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateAccessEntry",
        "eks:DeleteAccessEntry"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "eks:accessEntryType" : "STANDARD"
        },
        "ArnLike" : {
          "eks:principalArn" : "arn:aws:iam::*:role/aws-service-role/eks.amazonaws.com/
AWSServiceRoleForAmazonEKS"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/${aws:PrincipalAccount}/
AWSServiceRoleForAmazonEKS/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/${aws:PrincipalAccount}/
AWSServiceRoleForAmazonEKS/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "eks:policyArn" : [
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSComputePolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSComputeClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSNetworkingPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSNetworkingClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSLoadBalancingPolicy",
            "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSLoadBalancingClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSBlockStoragePolicy",
            "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSBlockStorageClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSHybridPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSEventPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSPodIdentityPolicy"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "eks:DescribeAccessEntry",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "eks:accessEntryType" : "EC2"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/EKS*",
```

```
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.ec2",
            "aws.health"
          ]
        },
        "StringEquals" : {
          "events:ManagedBy" : [
            "eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "events:PutTargets",
      "Resource" : "arn:aws:events:*:*:rule/EKS*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:ListInstanceProfiles"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "arn:aws:iam::*:instance-profile/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:TerminateInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:instance/*"
```

```
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:TerminateInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : [
            "eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteTargetGroup",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSVPCResourceController

Descrição: política usada pelo VPC Resource Controller para gerenciar ENI e IPs para nós de processamento.

`AmazonEKSVPCResourceController` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEKSVPCResourceController` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 12 de agosto de 2020, 0:55 UTC
- Hora da edição: 12 de agosto de 2020, 0:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "ec2:ResourceTag/eks:eni:owner" : "eks-vpc-resource-controller"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSWorkerNodeMinimalPolicy

Descrição: esta política permite que os nós de processamento do Amazon EKS se conectem aos clusters do Amazon EKS.

`AmazonEKSWorkerNodeMinimalPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEKSWorkerNodeMinimalPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 2 de outubro de 2024, 20:03 UTC
- Hora da edição: 2 de outubro de 2024, 20:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSWorkerNodeMinimalPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEKSWorkerNodePolicy

Descrição: esta política permite que os nós de processamento do Amazon EKS se conectem aos clusters do Amazon EKS.

`AmazonEKSWorkerNodePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEKSWorkerNodePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de maio de 2018, 21:09 UTC
- Hora da edição: 27 de novembro de 2023, 0:06 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "eks:DescribeCluster",
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElastiCacheFullAccess

Descrição: Fornece acesso total à Amazon ElastiCache por meio do Console de gerenciamento da AWS.

`AmazonElastiCacheFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElastiCacheFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 28 de novembro de 2023, 3:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : "elasticache:*",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/elasticache.amazonaws.com/
AWSServiceRoleForElastiCache",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticache.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateVPCEndpoints",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
        }
      }
    },
    {
      "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    },
    {
      "Sid" : "TagVPCEndpointsOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AmazonElastiCacheManaged" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "AllowAccessToEc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToAutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeLogGroups",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListLogDeliveryStreams",
      "Effect" : "Allow",
      "Action" : [
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToOutposts",
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToSNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElastiCacheReadOnlyAccess

Descrição: Fornece acesso somente para leitura à Amazon ElastiCache por meio do Console de gerenciamento da AWS.

`AmazonElastiCacheReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElastiCacheReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
```

```
        "elasticache:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticContainerRegistryPublicFullAccess

Descrição: fornece acesso administrativo a recursos públicos do Amazon ECR

`AmazonElasticContainerRegistryPublicFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticContainerRegistryPublicFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2020, 17:25 UTC
- Hora da edição: 01 de dezembro de 2020, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:*",
        "sts:GetServiceBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticContainerRegistryPublicPowerUser

Descrição: fornece acesso total aos repositórios públicos do Amazon ECR, mas não permite a exclusão de repositórios ou alterações de políticas.

`AmazonElasticContainerRegistryPublicPowerUser` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticContainerRegistryPublicPowerUser` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2020, 16:16 UTC
- Hora da edição: 01 de dezembro de 2020, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:DescribeRepositories",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:InitiateLayerUpload",
        "ecr-public:UploadLayerPart",
        "ecr-public:CompleteLayerUpload",
        "ecr-public:PutImage"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticContainerRegistryPublicReadOnly

Descrição: fornece acesso somente leitura a repositórios públicos do Amazon ECR.

`AmazonElasticContainerRegistryPublicReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticContainerRegistryPublicReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2020, 17:27 UTC
- Horário de edição: 01 de dezembro de 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:DescribeRepositories",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRegistryCatalogData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticFileSystemClientFullAccess

Descrição: concede acesso de cliente raiz a um sistema de arquivos do Amazon EFS

`AmazonElasticFileSystemClientFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticFileSystemClientFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 13 de janeiro de 2020, 16:27 UTC
- Hora da edição: 13 de janeiro de 2020, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticFileSystemClientReadOnlyAccess

Descrição: concede acesso de cliente somente leitura a um sistema de arquivos do Amazon EFS

`AmazonElasticFileSystemClientReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticFileSystemClientReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 13 de janeiro de 2020, 16:24 UTC
- Hora da edição: 13 de janeiro de 2020, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticFileSystemClientReadWriteAccess

Descrição: concede acesso de cliente de leitura e gravação a um sistema de arquivos do Amazon EFS

`AmazonElasticFileSystemClientReadWriteAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticFileSystemClientReadWriteAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 13 de janeiro de 2020, 16:21 UTC
- Hora da edição: 13 de janeiro de 2020, 16:21 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticFileSystemFullAccess

Descrição: Fornece acesso total ao Amazon EFS por meio do Console de gerenciamento da AWS.

`AmazonElasticFileSystemFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticFileSystemFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de maio de 2015, 16:22 UTC
- Horário editado: 07 de novembro de 2024, 19:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticFileSystemFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
```

```
        "ec2:ModifyNetworkInterfaceAttribute",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:CreateTags",
        "elasticfilesystem:CreateAccessPoint",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "elasticfilesystem:DeleteTags",
        "elasticfilesystem:DeleteAccessPoint",
        "elasticfilesystem:DeleteFileSystemPolicy",
        "elasticfilesystem:DeleteReplicationConfiguration",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:ModifyMountTargetSecurityGroups",
        "elasticfilesystem:PutAccountPreferences",
        "elasticfilesystem:PutBackupPolicy",
        "elasticfilesystem:PutLifecycleConfiguration",
        "elasticfilesystem:PutFileSystemPolicy",
        "elasticfilesystem:UpdateFileSystem",
        "elasticfilesystem:UpdateFileSystemProtection",
        "elasticfilesystem:TagResource",
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:ListTagsForResource",
        "elasticfilesystem:Backup",
        "elasticfilesystem:Restore",
        "elasticfilesystem:ReplicationRead",
        "elasticfilesystem:ReplicationWrite",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleForEFS",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "elasticfilesystem.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForEFS",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "elasticfilesystem.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticFileSystemReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon EFS por meio do Console de gerenciamento da AWS.

`AmazonElasticFileSystemReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticFileSystemReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de maio de 2015, 16:25 UTC
- Horário editado: 07 de novembro de 2024, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticFileSystemReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
```

```
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:ListTagsForResource",
        "elasticfilesystem:ReplicationRead",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticFileSystemServiceRolePolicy

Descrição: Permite que o Amazon Elastic File System gerencie AWS recursos em seu nome

`AmazonElasticFileSystemServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 05 de novembro de 2019, 16:52 UTC

- Horário editado: 07 de novembro de 2024, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:MountCapsule",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:ModifyNetworkInterfaceAttribute",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "backup:CreateBackupVault",
        "backup:PutBackupVaultAccessPolicy"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-vault:aws/efs/automatic-backup-vault"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupPlan",
        "backup:CreateBackupSelection"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-plan:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/backup.amazonaws.com/
AWSServiceRoleForBackup"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DeleteReplicationConfiguration",
        "elasticfilesystem:ReplicationRead",
        "elasticfilesystem:ReplicationWrite"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticFileSystemsUtils

Descrição: permite que os clientes usem o AWS Systems Manager para gerenciar automaticamente o pacote de utilitários do Amazon EFS (amazon-efs-utils) em suas instâncias do EC2 e usem CloudWatchLog para receber notificações de montagem do sistema de arquivos EFS. success/failure

`AmazonElasticFileSystemsUtils` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticFileSystemsUtils` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de setembro de 2020, 15:16 UTC
- Horário editado: 07 de abril de 2026, 13:12 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
```

```
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "efs-utils/S3Files",
            "efs-utils/EFS"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticMapReduceEditorsRole

Descrição: Política padrão para a função de serviço Amazon Elastic MapReduce Editors.

`AmazonElasticMapReduceEditorsRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticMapReduceEditorsRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 16 de novembro de 2018, 21:55 UTC
- Hora da edição: 09 de fevereiro de 2023, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListSteps"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : [
            "aws:elasticmapreduce:editor-id",
            "aws:elasticmapreduce:job-flow-id"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticMapReduceforAutoScalingRole

Descrição: Amazon Elastic MapReduce para Auto Scaling. Função para permitir que o ajuste de escacla automático adicione e remova instâncias do seu cluster EMR.

`AmazonElasticMapReduceforAutoScalingRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticMapReduceforAutoScalingRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 18 de novembro de 2016, 1:09 UTC
- Hora da edição: 18 de novembro de 2016, 1:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticMapReduceforEC2Role

Descrição: Política padrão para a função de serviço Amazon Elastic MapReduce for EC2.

`AmazonElasticMapReduceforEC2Role` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticMapReduceforEC2Role` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 11 de agosto de 2017, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "cloudwatch:*",
        "dynamodb:*",
        "ec2:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSteps",
        "kinesis:CreateStream",
        "kinesis:DeleteStream",
```

```
        "kinesis:DescribeStream",
        "kinesis:GetRecords",
        "kinesis:GetShardIterator",
        "kinesis:MergeShards",
        "kinesis:PutRecord",
        "kinesis:SplitShard",
        "rds:Describe*",
        "s3:*",
        "sdb:*",
        "sns:*",
        "sqs:*",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersions",
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:UpdatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:CreateUserDefinedFunction",
        "glue:UpdateUserDefinedFunction",
        "glue:DeleteUserDefinedFunction",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticMapReduceFullAccess

Descrição: esta política será descontinuada. Consulte a documentação para obter orientação: https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html. Fornece acesso total ao Amazon Elastic MapReduce e aos serviços subjacentes que ele exige, como EC2 e S3

`AmazonElasticMapReduceFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticMapReduceFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 11 de setembro de 2026, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Action" : [
        "cloudwatch:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateRoute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteRoute",
        "ec2:DeleteTags",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkAcls",
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "elasticmapreduce:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListRoles",
        "iam:PassRole",
        "kms:List*",
        "s3:*",
        "sdb:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "elasticmapreduce.amazonaws.com",
            "elasticmapreduce.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticMapReducePlacementGroupPolicy

Descrição: política para permitir que o EMR crie, descreva e exclua grupos de posicionamento do EC2.

`AmazonElasticMapReducePlacementGroupPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticMapReducePlacementGroupPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de setembro de 2020, 0:37 UTC
- Hora da edição: 29 de setembro de 2020, 0:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Resource" : "*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeletePlacementGroup",
```

```
        "ec2:DescribePlacementGroups"
      ]
    },
    {
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticMapReduceReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon Elastic MapReduce por meio do Console de gerenciamento da AWS.

`AmazonElasticMapReduceReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticMapReduceReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 29 de julho de 2020, 23:14 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "sdb:Select",
        "cloudwatch:GetMetricStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticMapReduceRole

Descrição: esta política será descontinuada. Consulte a documentação para obter orientação: Política https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html. padrão para a função de MapReduce serviço Amazon Elastic.

`AmazonElasticMapReduceRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticMapReduceRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 24 de junho de 2020, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateFleet",
```

```
        "ec2:CreateLaunchTemplate",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DeleteVolume",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
```

```
        "iam:PassRole",
        "s3:CreateBucket",
        "s3:Get*",
        "s3:List*",
        "sdb:BatchPutAttributes",
        "sdb:Select",
        "sqs:CreateQueue",
        "sqs:Delete*",
        "sqs:GetQueue*",
        "sqs:PurgeQueue",
        "sqs:ReceiveMessage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:Describe*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticsearchServiceRolePolicy

Descrição: Permita que o Amazon Elasticsearch Service acesse outros AWS serviços, como APIs de rede do EC2, em seu nome.

`AmazonElasticsearchServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 07 de julho de 2017, 0:15 UTC
- Horário editado: 22 de junho de 2026, 12:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973135",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973136",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ES"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973198",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
```

```
    {
      "Sid" : "Stmt1480452973199",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973200",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973201",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973149",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973150",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973194",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973202",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticTranscoder_FullAccess

Descrição: concede aos usuários acesso total ao Elastic Transcoder e o acesso aos serviços associados que são necessários para a funcionalidade completa do Elastic Transcoder.

`AmazonElasticTranscoder_FullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticTranscoder_FullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de abril de 2018, 18:59 UTC
- Hora da edição: 10 de junho de 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "elastictranscoder.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticTranscoder_JobsSubmitter

Descrição: concede aos usuários permissão para alterar predefinições, enviar trabalhos e visualizar as configurações do Elastic Transcoder. Esta política também concede acesso somente leitura a alguns outros serviços necessários para usar o console do Elastic Transcode, incluindo o S3, IAM e SNS.

`AmazonElasticTranscoder_JobsSubmitter` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticTranscoder_JobsSubmitter` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 07 de junho de 2018, 21:12 UTC
- Hora da edição: 10 de junho de 2019, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "elastictranscoder:*Job",
        "elastictranscoder:*Preset",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticTranscoder_ReadOnlyAccess

Descrição: concede aos usuários acesso somente de leitura ao Elastic Transcoder e acesso de lista a serviços relacionados.

`AmazonElasticTranscoder_ReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticTranscoder_ReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 07 de junho de 2018, 21:09 UTC
- Hora da edição: 10 de junho de 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
```

```
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonElasticTranscoderRole

Descrição: política padrão para o perfil de serviço do Amazon Elastic Transcoder.

`AmazonElasticTranscoderRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonElasticTranscoderRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 13 de junho de 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:Get*",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:*MultipartUpload*"
      ],
      "Sid" : "1",
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Sid" : "2",
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEMRCleanupPolicy

Descrição: Permite as ações que o EMR exige para encerrar e excluir recursos do AWS EC2 se a função de serviço do EMR perder essa capacidade.

`AmazonEMRCleanupPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 26 de setembro de 2017, 23:54 UTC
- Hora da edição: 29 de setembro de 2020, 21:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
```

```
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DeleteLaunchTemplate",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances",
        "ec2:CancelSpotInstanceRequests",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "ec2:DeleteVolume",
        "ec2:DescribePlacementGroups",
        "ec2:DeletePlacementGroup"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEMRContainersServiceRolePolicy

Descrição: Permite o acesso a outros recursos de AWS serviço necessários para executar o Amazon EMR

`AmazonEMRContainersServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Hora da criação: 09 de dezembro de 2020, 0:38 UTC
- Horário editado: 24 de julho de 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:ListNodeGroups",
        "eks:DescribeNodeGroup",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "acm:ImportCertificate",
        "acm:AddTagsToCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/emr-container:endpoint:managed-certificate" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:DeleteCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/emr-container:endpoint:managed-certificate" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointServiceCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint-service/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/emr-containers:managed-endpoint-resource" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointServiceManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:ModifyVpcEndpointServicePermissions"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint-service/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/emr-containers:managed-endpoint-resource" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointServiceTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint-service/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpointServiceConfiguration"
        }
      }
    },
    {
      "Sid" : "CloudWatchPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/EMRContainers"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEMRFullAccessPolicy_v2

Descrição: fornece acesso total ao Amazon EMR

`AmazonEMRFullAccessPolicy_v2` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEMRFullAccessPolicy_v2` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 12 de março de 2021, 1:50 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunJobFlowExplicitlyWithEMRManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:RunJobFlow"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddInstanceFleet",
        "elasticmapreduce:AddInstanceGroups",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:CreateEditor",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:CreateSecurityConfiguration",
        "elasticmapreduce:DeleteEditor",
        "elasticmapreduce:DeleteSecurityConfiguration",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeEditor",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:DescribePersistentAppUI",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeReleaseLabel",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetPersistentAppUIPresignedURL",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListEditors",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ModifyCluster",
        "elasticmapreduce:ModifyInstanceFleet",
        "elasticmapreduce:ModifyInstanceGroups",
        "elasticmapreduce:OpenEditorInConsole",
        "elasticmapreduce:PutAutoScalingPolicy",
        "elasticmapreduce:PutBlockPublicAccessConfiguration",
        "elasticmapreduce:PutManagedScalingPolicy",
```

```
        "elasticmapreduce:RemoveAutoScalingPolicy",
        "elasticmapreduce:RemoveManagedScalingPolicy",
        "elasticmapreduce:RemoveTags",
        "elasticmapreduce:SetTerminationProtection",
        "elasticmapreduce:StartEditor",
        "elasticmapreduce:StopEditor",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewMetricsInEMRConsole",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleForElasticMapReduce",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_DefaultRole_V2",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "elasticmapreduce.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForAutoScaling",
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticmapreduce.amazonaws.com*/AWSServiceRoleForEMRCleanup*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "elasticmapreduce.amazonaws.com",
            "elasticmapreduce.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleUIActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "s3:ListAllMyBuckets",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEMRReadOnlyAccessPolicy_v2

Descrição: Fornece acesso somente para leitura ao Amazon EMR e às CloudWatch métricas associadas.

`AmazonEMRReadOnlyAccessPolicy_v2` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEMRReadOnlyAccessPolicy_v2` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 12 de março de 2021, 1:39 UTC
- Hora da edição: 02 de agosto de 2023, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeEditor",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeReleaseLabel",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListEditors",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewMetricsInEMRConsole",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEMRServerlessServiceRolePolicy

Descrição: Permite o acesso a outros recursos AWS de serviço necessários para executar o Amazon EMRServerless

`AmazonEMRServerlessServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 20 de maio de 2022, 23:15 UTC
- Hora da edição: 25 de janeiro de 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2PolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/EMRServerless",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEMRServicePolicy_v2

Descrição: esta política é usada para o perfil de serviço do Amazon EMR e NÃO deve ser usada para nenhum outro usuário ou perfil do IAM em sua conta. A política concede permissões para criar e gerenciar recursos associados ao EMR e serviços relacionados necessários para a operação do seu cluster do EMR.

`AmazonEMRServicePolicy_v2` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEMRServicePolicy_v2` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 12 de março de 2021, 1:11 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "CreateInTaggedNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateWithEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "CreateEMRTaggedInstancesAndVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ResourcesToLaunchEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/ami-*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*:*:placement-group/EMR_*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:dedicated-host/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    },
    {
      "Sid" : "ManageEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
```

```
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ManageTagsOnEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaceNeededForPrivateSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "TagOnCreateTaggedEMRResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateFleet",
            "CreateLaunchTemplate",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "TagPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:placement-group/EMR_*"
      ]
    },
    {
      "Sid" : "ListActionsForEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
```

```
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateDefaultSecurityGroupInVPCWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "TagOnCreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "ManageSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*"
    },
    {
      "Sid" : "DeletePlacementGroups",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeletePlacementGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsForCapacityReservations",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*_EMR_Auto_Scaling"
    },
    {
      "Sid" : "PassRoleForAutoScaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
```

```
        }
      }
    },
    {
      "Sid" : "PassRoleForEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "CreateAndModifyEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "aws:RequestTag/Name" : "emr-service-vpce"
        }
      }
    },
    {
      "Sid" : "TagEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "aws:RequestTag/Name" : "emr-service-vpce"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEMRServicePolicyForSessions

Descrição: Fornece permissões para provisionar e gerenciar balanceadores de carga de rede, serviços de endpoint de VPC e grupos de segurança necessários para sessões interativas do Amazon EMR Spark Connect no EMR em clusters do EC2.

`AmazonEMRServicePolicyForSessions` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEMRServicePolicyForSessions` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 22 de junho de 2026, 19:57 UTC
- Horário editado: 22 de junho de 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicyForSessions`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NLBProvisioning",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*",
        "arn:aws:elasticloadbalancing:*:*:listener/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "NLBManagement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:SetSecurityGroups",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*",
        "arn:aws:elasticloadbalancing:*:*:listener/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "NLBDescribes",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "VPCEndpointServiceProvisioning",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint-service/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointServiceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:ModifyVpcEndpointServicePermissions"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint-service/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointServiceDescribes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagOnCreateEndpointServiceResources",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint-service/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpcEndpointServiceConfiguration"
          ]
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRoleForELB",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityGroupProvisioning",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupCreateInVpc",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
```

```
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonESCognitoAccess

Descrição: fornece acesso limitado ao serviço de configuração do Amazon Cognito.

`AmazonESCognitoAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonESCognitoAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de fevereiro de 2018, 22:29 UTC
- Hora da edição: 20 de dezembro de 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESCognitoAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:AdminInitiateAuth",
        "cognito-idp:AdminUserGlobalSignOut",
        "cognito-idp:ListUserPoolClients",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:UpdateIdentityPool",
        "cognito-identity:SetIdentityPoolRoles",
        "cognito-identity:GetIdentityPoolRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com",
            "cognito-identity-us-gov.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonESFullAccess

Descrição: fornece acesso total ao serviço de configuração do Amazon ES.

`AmazonESFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonESFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de outubro de 2015, 19:14 UTC
- Hora da edição: 01 de outubro de 2015, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "es:*"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonESReadOnlyAccess

Descrição: fornece acesso somente leitura ao serviço de configuração do Amazon ES.

`AmazonESReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonESReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de outubro de 2015, 19:18 UTC
- Hora da edição: 3 de outubro de 2018, 3:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "es:Describe*",
        "es:List*",
        "es:Get*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEventBridgeApiDestinationsServiceRolePolicy

Descrição: Permite EventBridge acessar os recursos do Secret Manager em seu nome.

`AmazonEventBridgeApiDestinationsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 11 de fevereiro de 2021, 20:52 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" : [
            "arn:aws:secretsmanager:*:*:secret:events!connection/*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/EventBridgeApiDestinations" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEventBridgeFullAccess

Descrição: Fornece acesso total à Amazon EventBridge.

`AmazonEventBridgeFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEventBridgeFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de julho de 2019, 14:08 UTC

- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "schemas.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccessForApiDestinations",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!*"
    },
    {
      "Sid" : "IAMPassRoleAccessForEventBridge",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForScheduler",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEventBridgePipesFullAccess

Descrição: Fornece acesso total ao Amazon EventBridge Pipes.

`AmazonEventBridgePipesFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEventBridgePipesFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2022, 17:03 UTC
- Hora da edição: 01 de dezembro de 2022, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgePipesActions",
      "Effect" : "Allow",
      "Action" : "pipes:*",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEventBridgePipesOperatorAccess

Descrição: Fornece acesso somente de leitura e de operador (capacidade de parar e iniciar a execução de Pipes) ao Amazon EventBridge Pipes.

`AmazonEventBridgePipesOperatorAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEventBridgePipesOperatorAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2022, 17:04 UTC
- Hora da edição: 1º de dezembro de 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEventBridgePipesReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon EventBridge Pipes.

`AmazonEventBridgePipesReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEventBridgePipesReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2022, 17:04 UTC
- Hora da edição: 1º de dezembro de 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEventBridgeReadOnlyAccess

Descrição: Fornece acesso somente para leitura à Amazon EventBridge.

`AmazonEventBridgeReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEventBridgeReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de julho de 2019, 13:59 UTC

- Horário editado: 24 de setembro de 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:TestEventPattern",
        "events:DescribeArchive",
        "events:ListArchives",
        "events:DescribeReplay",
        "events:ListReplays",
        "events:DescribeConnection",
        "events:ListConnections",
        "events:DescribeApiDestination",
        "events:ListApiDestinations",
        "events:DescribeEndpoint",
        "events:ListEndpoints",
        "events:DescribeSubscriber",
        "events:ListSubscribers",
        "events:GetResourcePolicy",
        "events:ListResourcePolicies",
```

```
        "events:ListTagsForResource",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:ExportSchema",
        "schemas:GetCodeBindingSource",
        "schemas:GetDiscoveredSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "schemas:SearchSchemas",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEventBridgeSchedulerFullAccess

Descrição: A política AmazonEventBridgeSchedulerFullAccess gerenciada concede permissões para usar todas as ações do EventBridge Agendador para agendas e grupos de agendamentos.

`AmazonEventBridgeSchedulerFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEventBridgeSchedulerFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 10 de novembro de 2022, 18:37 UTC
- Horário editado: 12 de fevereiro de 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "scheduler:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEventBridgeSchedulerReadOnlyAccess

Descrição: A política AmazonEventBridgeSchedulerReadOnlyAccess gerenciada concede permissões somente de leitura para visualizar detalhes sobre suas agendas e grupos de agendamentos.

`AmazonEventBridgeSchedulerReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEventBridgeSchedulerReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 10 de novembro de 2022, 18:50 UTC
- Horário editado: 02 de abril de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:List*",
        "scheduler:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEventBridgeSchemasFullAccess

Descrição: Fornece acesso total aos EventBridge esquemas da Amazon.

`AmazonEventBridgeSchemasFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEventBridgeSchemasFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2019, 23:12 UTC
- Hora da edição: 28 de novembro de 2019, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEventBridgeSchemasFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "schemas:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEventBridgeManageRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
```

```
      "Resource" : "arn:aws:events:*:*:rule/*Schemas*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEventBridgeSchemasReadOnlyAccess

Descrição: Fornece acesso somente para leitura aos EventBridge esquemas da Amazon.

`AmazonEventBridgeSchemasReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonEventBridgeSchemasReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2019, 23:05 UTC
- Hora da edição: 01 de maio de 2020, 0:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEventBridgeSchemasReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "schemas:ListDiscoverers",
        "schemas:DescribeDiscoverer",
        "schemas:ListRegistries",
        "schemas:DescribeRegistry",
        "schemas:SearchSchemas",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:DescribeSchema",
        "schemas:GetDiscoveredSchema",
        "schemas:DescribeCodeBinding",
        "schemas:GetCodeBindingSource",
        "schemas:ListTagsForResource",
        "schemas:GetResourcePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEventBridgeSchemasServiceRolePolicy

Descrição: Concede permissões às regras gerenciadas criadas pelos EventBridge esquemas da Amazon.

`AmazonEventBridgeSchemasServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 27 de novembro de 2019, 1:10 UTC
- Hora da edição: 27 de novembro de 2019, 1:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/*Schemas-*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonEVSServiceRolePolicy

Descrição: concede permissões ao EVS para gerenciar recursos em seu nome.

`AmazonEVSServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 16 de maio de 2025, 23:37 UTC
- Horário editado: 22 de março de 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEVSServiceRolePolicy`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "ManageSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSubnet"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CreateEniWithTagStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "TagOnCreateNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonEVSManaged" : "false"
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "ManageEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AssignIpv6Addresses"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ManageInstanceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeInstanceAndVolumeStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageVolumeStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "ManageSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "UpdateSecurityGroupStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "CloudWatchPutMetricDataStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Usage",
            "AWS/EVS"
          ]
        }
      }
    },
    {
      "Sid" : "AccessSecretStatement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/EvsAccess" : "false"
        }
      }
    },
    {
      "Sid" : "DecryptSecretWithKmsKeyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:*:secret:*",
          "kms:EncryptionContext:SecretVersionId" : "*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/EvsAccess" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeKmsKeyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
```

```
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/EvsAccess" : "false"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonFISServiceRolePolicy

Descrição: Política para permitir que o AWS FIS gerencie o monitoramento e a seleção de recursos para experimentos.

`AmazonFISServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 21 de dezembro de 2020, 21:18 UTC
- Hora da edição: 25 de outubro de 2022, 9:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "fis.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventBridgeDescribe",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Tagging",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmHistory"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeUserResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "iam:GetUser",
        "iam:GetRole",
        "iam:ListUsers",
        "iam:ListRoles",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "ecs:DescribeClusters",
        "ecs:DescribeTasks",
        "ecs:ListTasks",
        "eks:DescribeNodegroup",
        "eks:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonForecastFullAccess

Descrição: concede acesso a todas as ações do Amazon Forecast

`AmazonForecastFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonForecastFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de janeiro de 2019, 1:52 UTC
- Hora da edição: 18 de janeiro de 2019, 1:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonForecastFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "forecast:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonFraudDetectorFullAccessPolicy

Descrição: concede acesso a todas as ações para o Amazon Fraud Detector

`AmazonFraudDetectorFullAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonFraudDetectorFullAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 03 de dezembro de 2019, 22:46 UTC
- Hora da edição: 03 de dezembro de 2019, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "frauddetector:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListEndpoints",
        "sagemaker:DescribeEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "frauddetector.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonFreeRTOSFullAccess

Descrição: política de acesso total para Amazon FreeRTOS

`AmazonFreeRTOSFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonFreeRTOSFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2017, 15:32 UTC
- Hora da edição: 29 de novembro de 2017, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "freertos:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonFreeRTOSOTAUpdate

Descrição: permite que o usuário acesse a atualização OTA do Amazon FreeRTOS

`AmazonFreeRTOSOTAUpdate` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonFreeRTOSOTAUpdate` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 27 de agosto de 2018, 22:43 UTC
- Hora da edição: 18 de dezembro de 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::afr-ota*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "signer:StartSigningJob",
        "signer:DescribeSigningJob",
        "signer:GetSigningProfile",
        "signer:PutSigningProfile"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteJob",
        "iot:DescribeJob"
      ],
      "Resource" : "arn:aws:iot:*:*:job/AFR_OTA*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteStream"
      ],
      "Resource" : "arn:aws:iot:*:*:stream/AFR_OTA*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateStream",
        "iot:CreateJob"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonFSxConsoleFullAccess

Descrição: Fornece acesso total ao Amazon FSx e acesso aos AWS serviços relacionados por meio do Console de gerenciamento da AWS.

`AmazonFSxConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonFSxConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2018, 16:36 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

Versão da política

Versão da política: v20 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListResourcesAssociatedWithFSxFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "kms:ListAliases",
        "logs:DescribeLogGroups",
        "s3:ListBucket",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateAndAttachS3AccessPoint",
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DeleteBackup",
        "fsx:DeleteDataRepositoryAssociation",
        "fsx:DeleteFileCache",
        "fsx:DeleteFileSystem",
        "fsx:DeleteSnapshot",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume",
        "fsx:DescribeAssociatedFileGateways",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeDataRepositoryTasks",
```

```
        "fsx:DescribeFileCaches",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeFileSystems",
        "fsx:DescribeS3AccessPointAttachments",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DetachAndDeleteS3AccessPoint",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateFSxSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
```

```
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonFSxConsoleReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon FSx e acesso a AWS serviços relacionados por meio do Console de gerenciamento da AWS.

`AmazonFSxConsoleReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonFSxConsoleReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2018, 16:35 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FSxReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "fsx:Describe*",
        "fsx:ListTagsForResource",
        "kms:DescribeKey",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonFSxFullAccess

Descrição: Fornece acesso total ao Amazon FSx e acesso aos AWS serviços relacionados.

`AmazonFSxFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonFSxFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2018, 16:34 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxFullAccess`

Versão da política

Versão da política: v13 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ViewAWSDSDirectories",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
```

```
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateAndAttachS3AccessPoint",
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DetachAndDeleteS3AccessPoint",
        "fsx:DeleteBackup",
        "fsx:DeleteDataRepositoryAssociation",
        "fsx:DeleteFileCache",
        "fsx:DeleteFileSystem",
        "fsx:DeleteSnapshot",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume",
        "fsx:DescribeAssociatedFileGateways",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeDataRepositoryTasks",
        "fsx:DescribeFileCaches",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeFileSystems",
        "fsx:DescribeS3AccessPointAttachments",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
```

```
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLRForFSx",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateLogsForFSxWindowsAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/fsx/*"
```

```
      ]
    },
    {
      "Sid" : "WriteToAmazonKinesisDataFirehose",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
      ]
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeEC2VpcResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonFSxReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon FSx.

`AmazonFSxReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonFSxReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2018, 16:33 UTC
- Hora da edição: 28 de novembro de 2018, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:Describe*",
        "fsx:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonFSxServiceRolePolicy

Descrição: Permite que o Amazon FSx gerencie AWS recursos em seu nome

`AmazonFSxServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 28 de novembro de 2018, 10:38 UTC
- Horário editado: 22 de julho de 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateFileSystem",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:GetAuthorizedApplicationDetails",
        "ds:UnauthorizeApplication",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAddresses",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:GetSecurityGroupsForVpc",
        "route53:AssociateVPCWithHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PutMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/FSx"
        }
      }
    },
    {
      "Sid" : "TagResourceNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "AmazonFSx.FileSystemId"
        }
      }
    },
    {
      "Sid" : "ManageNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonFSx.FileSystemId" : "false"
        }
      }
    },
    {
      "Sid" : "ManageRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRoute",
        "ec2:ReplaceRoute",
        "ec2:DeleteRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonFSx" : "ManagedByAmazonFSx"
        }
      }
```

```
    },
    {
      "Sid" : "PutCloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/fsx/*"
    },
    {
      "Sid" : "ManageAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonGlacierFullAccess

Descrição: Fornece acesso total ao Amazon Glacier por meio do Console de gerenciamento da AWS.

`AmazonGlacierFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonGlacierFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "glacier:*",
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonGlacierReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon Glacier por meio do Console de gerenciamento da AWS.

`AmazonGlacierReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonGlacierReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 5 de maio de 2016, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glacier:DescribeJob",
        "glacier:DescribeVault",
        "glacier:GetDataRetrievalPolicy",
        "glacier:GetJobOutput",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultLock",
```

```
        "glacier:GetVaultNotifications",
        "glacier:ListJobs",
        "glacier:ListMultipartUploads",
        "glacier:ListParts",
        "glacier:ListTagsForVault",
        "glacier:ListVaults"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonGrafanaAthenaAccess

Descrição: esta política concede acesso ao Amazon Athena e às dependências necessárias para permitir a consulta e a gravação de resultados no S3 a partir do plug-in Amazon Athena no Amazon Grafana.

`AmazonGrafanaAthenaAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonGrafanaAthenaAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 22 de novembro de 2021, 17:11 UTC
- Hora da edição: 22 de novembro de 2021, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetWorkGroup",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GrafanaDataSource" : "false"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::grafana-athena-query-results-*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonGrafanaCloudWatchAccess

Descrição: Essa política concede acesso à Amazon CloudWatch e às dependências necessárias para uso CloudWatch como fonte de dados no Amazon Managed Grafana.

`AmazonGrafanaCloudWatchAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonGrafanaCloudWatchAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 24 de março de 2023, 22:41 UTC
- Hora da edição: 24 de março de 2023, 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarmHistory",
```

```
        "cloudwatch:DescribeAlarms",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetInsightRuleReport"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:GetLogGroupFields",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:GetLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks",
        "oam:ListAttachedLinks"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonGrafanaRedshiftAccess

Descrição: esta política concede acesso limitado ao Amazon Redshift e às dependências necessárias para usar o plug-in do Amazon Redshift no Amazon Grafana.

`AmazonGrafanaRedshiftAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonGrafanaRedshiftAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 26 de novembro de 2021, 23:15 UTC
- Hora da edição: 26 de novembro de 2021, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:ListTables",
        "redshift-data:ListSchemas"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GrafanaDataSource" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbname:*/*",
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "secretsmanager:ResourceTag/RedshiftQueryOwner" : "false"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonGrafanaServiceLinkedRolePolicy

Descrição: Fornece acesso aos AWS recursos gerenciados ou usados pelo Amazon Grafana.

`AmazonGrafanaServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 08 de novembro de 2022, 23:10 UTC
- Hora da edição: 08 de novembro de 2022, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonGrafanaManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
```

```
        },
        "Null" : {
          "aws:RequestTag/AmazonGrafanaManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AmazonGrafanaManaged" : "false"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonGuardDutyFullAccess

Descrição: Fornece acesso total para usar a Amazon GuardDuty.

`AmazonGuardDutyFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonGuardDutyFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2017, 22:31 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonGuardDutyFullAccessSid1",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ActionsForOrganizationsSid1",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
```

```
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamGetRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    },
    {
      "Sid" : "AllowPassRoleToMalwareProtection",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "malware-protection-plan.guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonGuardDutyFullAccess_v2

Descrição: Fornece acesso total para usar a Amazon GuardDuty

`AmazonGuardDutyFullAccess_v2` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonGuardDutyFullAccess_v2` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 04 de junho de 2025, 20:22 UTC
- Horário editado: 28 de setembro de 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess_v2`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyFullAccess",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateGuardDutyServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
```

```
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyOrganizationsAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyIamRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
```

```
      "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    },
    {
      "Sid" : "AllowPassRoleToMalwareProtection",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "malware-protection-plan.guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonGuardDutyMalwareProtectionServiceRolePolicy

Descrição: a proteção contra GuardDuty malware usa a função vinculada ao serviço (SLR) chamada. AWSServiceRoleForAmazonGuardDutyMalwareProtection Essa função vinculada ao serviço permite que a proteção contra GuardDuty malware realize escaneamentos sem agente para detectar malware. Ele permite GuardDuty criar instantâneos em sua conta e compartilhar os instantâneos com a conta de GuardDuty serviço para verificar se há malware. Ele avalia esses instantâneos compartilhados e inclui os metadados da instância EC2 recuperados nas descobertas da Proteção contra Malware. GuardDuty A função AWSServiceRoleForAmazonGuardDutyMalwareProtection

vinculada ao serviço confia no serviço malware-protection.guardduty.amazonaws.com para assumir a função.

`AmazonGuardDutyMalwareProtectionServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 19 de julho de 2022, 19:06 UTC
- Hora da edição: 25 de janeiro de 2024, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeAndListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
```

```
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTasks",
        "ecs:DescribeTasks",
        "eks:DescribeCluster"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSnapshotVolumeConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyScanId"
        }
      }
    },
    {
      "Sid" : "CreateTagsPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:*/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    },
    {
      "Sid" : "AddTagsToSnapshotPermission",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/GuardDutyScanId" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "GuardDutyExcluded",
            "GuardDutyFindingDetected"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteAndShareSnapshotPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/GuardDutyScanId" : "*"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "PreventPublicAccessToSnapshotPermission",
      "Effect" : "Deny",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/group" : "all"
        }
      }
    },
```

```
    {
      "Sid" : "CreateGrantPermission",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "snap-*"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "CreateGrant",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "ShareSnapshotKMSPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "DescribeKeyPermission",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "GuardDutyLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
    },
    {
      "Sid" : "GuardDutyLogStreamPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
    },
    {
      "Sid" : "EBSDirectAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:GetSnapshotBlock",
        "ebs:ListSnapshotBlocks"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/GuardDutyScanId" : "*"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    }
```

```
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonGuardDutyReadOnlyAccess

Descrição: Fornece acesso somente para leitura aos GuardDuty recursos da Amazon

`AmazonGuardDutyReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonGuardDutyReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2017, 22:29 UTC
- Hora da edição: 16 de novembro de 2023, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonGuardDutyServiceRolePolicy

Descrição: Habilite o acesso aos AWS recursos usados ou gerenciados pelo Amazon Guard Duty

`AmazonGuardDutyServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 28 de novembro de 2017, 20:12 UTC
- Horário editado: 09 de setembro de 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

Versão da política

Versão da política: v13 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyGetDescribeListPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeTransitGatewayAttachments",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
```

```
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ecs:ListClusters",
        "ecs:DescribeClusters",
        "ecs:DescribeTasks",
        "ecs:DescribeTaskDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyCreateSLRPolicy",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        },
        "StringLike" : {
```

```
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.guardduty-data",
            "com.amazonaws.*.guardduty-data-fips"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyModifyDeleteVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAnyValue:StringEquals" : {
```

```
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutySecurityGroupManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/GuardDutyManaged" : "*"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupForVpcPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateEksAddonPolicy",
      "Effect" : "Allow",
      "Action" : "eks:CreateAddon",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyEksAddonManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeleteAddon",
        "eks:UpdateAddon",
        "eks:DescribeAddon"
      ],
      "Resource" : "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
    },
    {
      "Sid" : "GuardDutyEksClusterTagResourcePolicy",
      "Effect" : "Allow",
      "Action" : "eks:TagResource",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyEcsPutAccountSettingsDefaultPolicy",
      "Effect" : "Allow",
      "Action" : "ecs:PutAccountSettingDefault",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:account-setting" : [
            "guardDutyActivate"
          ]
        }
      }
    },
    {
      "Sid" : "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:DeleteAssociation",
        "ssm:UpdateAssociation",
        "ssm:CreateAssociation",
        "ssm:StartAssociationsOnce"
      ],
      "Resource" : "arn:aws:ssm:*:*:association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/GuardDutyManaged" : "true"
        }
      }
    },
    {
      "Sid" : "SsmAddTagsToResourcePermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:association/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "GuardDutyManaged"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/GuardDutyManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "SsmCreateUpdateAssociationInstanceDocumentPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
    },
    {
      "Sid" : "SsmSendCommandPermission",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin"
      ]
    },
    {
      "Sid" : "SsmGetCommandStatus",
      "Effect" : "Allow",
      "Action" : "ssm:GetCommandInvocation",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudTrailCreateServiceLinkedChannelSid",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/guardduty/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GdLatticeCreateManagedSnvaAssociation",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:CreateServiceNetworkVpcAssociation",
      "Resource" : "arn:aws:vpc-lattice:*:*:servicenetworkvpcassociation/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GdLatticeAssociateViaAwsService",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:AssociateViaAWSService",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonHealthLakeFullAccess

Descrição: Fornece acesso total ao HealthLake serviço da Amazon.

`AmazonHealthLakeFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonHealthLakeFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de fevereiro de 2021, 1:07 UTC
- Hora da edição: 17 de fevereiro de 2021, 1:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "healthlake:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "healthlake.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonHealthLakeReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao HealthLake serviço da Amazon.

`AmazonHealthLakeReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonHealthLakeReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de fevereiro de 2021, 2:43 UTC
- Horário editado: 04 de agosto de 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "healthlake:ListFHIRDatastores",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:GetCapabilities",
```

```
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost",
        "healthlake:GetDataTransformationProfile",
        "healthlake:ListDataTransformationProfiles",
        "healthlake:ListDataTransformationProfileVersions",
        "healthlake:DescribeDataTransformationJob",
        "healthlake:ListDataTransformationJobs",
        "healthlake:ValidateSource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonHoneycodeFullAccess

Descrição: Fornece acesso total ao Honeycode por meio do Console de gerenciamento da AWS e do SDK.

`AmazonHoneycodeFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonHoneycodeFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de junho de 2020, 20:28 UTC
- Hora da edição: 24 de junho de 2020, 20:28 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:*"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonHoneycodeReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Honeycode por meio do Console de gerenciamento da AWS e do SDK.

`AmazonHoneycodeReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonHoneycodeReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de junho de 2020, 20:28 UTC
- Hora da edição: 1º de dezembro de 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:List*",
        "honeycode:Get*",
        "honeycode:Describe*",
        "honeycode:Query*"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonHoneycodeServiceRolePolicy

Descrição: um perfil vinculado ao serviço necessário para que o Amazon Honeycode acesse seus recursos.

`AmazonHoneycodeServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 18 de novembro de 2020, 18:03 UTC
- Hora da edição: 18 de novembro de 2020, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sso:GetManagedApplicationInstance"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonHoneycodeTeamAssociationFullAccess

Descrição: Fornece acesso total à Honeycode Team Association por meio do Console de gerenciamento da AWS e do SDK.

`AmazonHoneycodeTeamAssociationFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonHoneycodeTeamAssociationFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de junho de 2020, 20:28 UTC
- Hora da edição: 24 de junho de 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:ListTeamAssociations",
        "honeycode:ApproveTeamAssociation",
        "honeycode:RejectTeamAssociation"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonHoneycodeTeamAssociationReadOnlyAccess

Descrição: Fornece acesso somente para leitura à Honeycode Team Association por meio do Console de gerenciamento da AWS e do SDK.

`AmazonHoneycodeTeamAssociationReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonHoneycodeTeamAssociationReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de junho de 2020, 20:27 UTC
- Hora da edição: 24 de junho de 2020, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:ListTeamAssociations"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonHoneycodeWorkbookFullAccess

Descrição: Fornece acesso total à pasta de trabalho Honeycode por meio do Console de gerenciamento da AWS e do SDK.

`AmazonHoneycodeWorkbookFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonHoneycodeWorkbookFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de junho de 2020, 20:28 UTC
- Hora da edição: 01 de dezembro de 2020, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
```

```
        "honeycode:InvokeScreenAutomation",
        "honeycode:BatchCreateTableRows",
        "honeycode:BatchDeleteTableRows",
        "honeycode:BatchUpdateTableRows",
        "honeycode:BatchUpsertTableRows",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows",
        "honeycode:StartTableDataImportJob"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonHoneycodeWorkbookReadOnlyAccess

Descrição: Fornece acesso somente para leitura à pasta de trabalho Honeycode por meio do Console de gerenciamento da AWS e do SDK.

`AmazonHoneycodeWorkbookReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonHoneycodeWorkbookReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 24 de junho de 2020, 20:28 UTC
- Hora da edição: 01 de dezembro de 2020, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonInspector2AgentlessServiceRolePolicy

Descrição: Concede ao Amazon Inspector o acesso Serviços da AWS necessário para realizar avaliações de segurança sem agentes

`AmazonInspector2AgentlessServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 20 de novembro de 2023, 15:18 UTC
- Horário editado: 20 de agosto de 2026, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstanceIdentification",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
```

```
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetSnapshotData",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InspectorScan" : "*"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAnyInstanceOrVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "DenyCreateSnapshotsOnExcludedInstances",
      "Effect" : "Deny",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/InspectorEc2Exclusion" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsOnAnySnapshotOnlyWithTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
```

```
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "InspectorScan"
        }
      }
    },
    {
      "Sid" : "CreateOnlyInspectorScanTagOnlyUsingCreateSnapshots",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : "CreateSnapshots"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "InspectorScan"
        }
      }
    },
    {
      "Sid" : "DeleteOnlySnapshotsTaggedForScanning",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/InspectorScan" : "*"
        }
      }
    },
    {
      "Sid" : "DenyKmsDecryptForExcludedKeys",
      "Effect" : "Deny",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/InspectorEc2Exclusion" : "true"
        }
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksVolContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "vol-*"
        }
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksSnapContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "snap-*"
        }
      }
    },
    {
      "Sid" : "DescribeKeysForEbsOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DecryptCrossAccountOrgVolContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "vol-*"
        }
      }
    },
    {
      "Sid" : "DecryptCrossAccountOrgSnapContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "snap-*"
        }
      }
    },
    {
      "Sid" : "DescribeCrossAccountOrgKeysForEbsOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListKeyResourceTags",
      "Effect" : "Allow",
      "Action" : "kms:ListResourceTags",
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonInspector2AmiScanServiceRolePolicy

Descrição: Concede ao Amazon Inspector o acesso Serviços da AWS necessário para realizar avaliações de segurança para a AMI

`AmazonInspector2AmiScanServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 30 de julho de 2026, 17:57 UTC
- Horário editado: 30 de julho de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AmiScanServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
      ]
    },
    {
      "Sid" : "AllowInspectorEnablementForAwsOrgPolicy",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:AssociateMember",
        "inspector2:Disable",
        "inspector2:Enable",
        "inspector2:EnableDelegatedAdminAccount"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowInspectorServiceGetAwsOrg",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowInspectorServiceDelegatedAdminFromAwsOrg",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "ami.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmiIdentification",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetSnapshotData",
      "Effect" : "Allow",
      "Action" : [
        "ebs:GetSnapshotBlock",
        "ebs:ListSnapshotBlocks"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Sid" : "DenyGetSnapshotDataOnExcludedSnapshots",
      "Effect" : "Deny",
```

```
      "Action" : [
        "ebs:GetSnapshotBlock",
        "ebs:ListSnapshotBlocks"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/InspectorEc2Exclusion" : "true"
        }
      }
    },
    {
      "Sid" : "DenyKmsDecryptForExcludedKeys",
      "Effect" : "Deny",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/InspectorEc2Exclusion" : "true"
        }
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksVolContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "vol-*",
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksSnapContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "snap-*",
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DescribeKeysForEbsOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListKeyResourceTags",
      "Effect" : "Allow",
      "Action" : "kms:ListResourceTags",
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonInspector2FullAccess

Descrição: fornece acesso total ao Amazon Inspector e acesso a outros serviços relacionados, como organizações.

`AmazonInspector2FullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonInspector2FullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2021, 19:10 UTC
- Hora da edição: 25 de abril de 2024, 13:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFullAccessToInspectorApis",
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCodeGuruApis",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCreateSlr",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonInspector2FullAccess_v2

Descrição: fornece acesso total ao Amazon Inspector e a outros serviços relacionados, como as organizações com acesso organizacional restritivo.

`AmazonInspector2FullAccess_v2` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonInspector2FullAccess_v2` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de julho de 2025, 16:07 UTC
- Horário editado: 08 de julho de 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess_v2`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFullAccessToInspectorApis",
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCodeGuruApis",
      "Effect" : "Allow",
```

```
      "Action" : [
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCreateSlr",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com",
            "thirdparty.inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowServicePrincipalBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "inspector2.amazonaws.com",
            "agentless.inspector2.amazonaws.com",
            "thirdparty.inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOrganizationalBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "arn:aws:organizations::*:ou/o-*/ou-*"
    },
    {
      "Sid" : "AllowAccountsBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : "arn:aws:organizations::*:account/o-*/*"
    },
    {
      "Sid" : "AllowAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListPoliciesForInspectorPolicyType",
      "Effect" : "Allow",
      "Action" : "organizations:ListPolicies",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDescribeResourcePolicyForDelegation",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeResourcePolicy",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDescribeEffectivePolicyForInspector",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeEffectivePolicy",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "AllowConfigConnectorWriteAndList",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConnector",
        "config:ListConnectors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowConfigConnectorRead",
      "Effect" : "Allow",
      "Action" : "config:GetConnector",
      "Resource" : "arn:aws:config:*:*:connector/*"
    },
    {
      "Sid" : "AllowCreateConfigThirdPartySLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
thirdparty.config.amazonaws.com/AWSServiceRoleForConfigThirdParty",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "thirdparty.config.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonInspector2ManagedCisPolicy

Descrição: esta é uma política gerenciada que o cliente deve anexar a seus perfis para se comunicar com o serviço de inspeção para verificações de CIS

`AmazonInspector2ManagedCisPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonInspector2ManagedCisPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de janeiro de 2024, 16:31 UTC
- Hora da edição: 24 de janeiro de 2024, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
```

```
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonInspector2ManagedTelemetryPolicy

Descrição: Concede permissões para se comunicar com o Inspector2 Telemetry Channel

`AmazonInspector2ManagedTelemetryPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonInspector2ManagedTelemetryPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 13 de fevereiro de 2026, 17:12 UTC
- Horário editado: 13 de fevereiro de 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedTelemetryPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForInspector2Telemetry",
      "Effect" : "Allow",
      "Action" : [
        "inspector2-telemetry:StartSession",
        "inspector2-telemetry:StopSession",
        "inspector2-telemetry:SendTelemetry",
        "inspector2-telemetry:NotifyHeartbeat"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonInspector2ReadOnlyAccess

Descrição: fornece acesso somente de leitura ao serviço Amazon Inspector2 e aos serviços de suporte relevantes

`AmazonInspector2ReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonInspector2ReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 21 de janeiro de 2022, 14:45 UTC
- Horário editado: 07 de julho de 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "inspector2:BatchGet*",
        "inspector2:List*",
        "inspector2:Describe*",
        "inspector2:Get*",
        "inspector2:Search*",
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListPoliciesForInspectorPolicyType",
      "Effect" : "Allow",
      "Action" : "organizations:ListPolicies",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDescribeResourcePolicyForDelegation",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeResourcePolicy",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDescribeEffectivePolicyForInspector",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeEffectivePolicy",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCrossServiceReadsForConnectorHealth",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:ListConfigurationRecorders",
        "config:GetConnector",
        "config:ListConnectors",
        "ssm:GetCloudConnector",
```

```
        "ssm:ListCloudConnectors"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonInspector2ServiceRolePolicy

Descrição: Concede ao Amazon Inspector o acesso Serviços da AWS necessário para realizar avaliações de segurança

`AmazonInspector2ServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 16 de novembro de 2021, 20:27 UTC
- Horário editado: 16 de junho de 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

Versão da política

Versão da política: v27 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TirosPolicy",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTables",
```

```
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:GetTransitGatewayPolicyTableEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallMetadata",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PackageVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImages",
```

```
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:ListImages",
        "ecr:PutRegistryScanningConfiguration",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "ssm:DescribeAssociation",
        "ssm:DescribeAssociationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:ListAssociations",
        "ssm:ListResourceDataSync"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaPackageVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions",
        "lambda:GetFunction",
        "lambda:GetLayerVersion",
        "lambda:ListTags",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GatherInventory",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:StartAssociationsOnce",
        "ssm:UpdateAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AmazonInspector2-*",
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*:*:managed-instance/*",
```

```
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "GatherInventoryDeleteAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "DataSyncCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateResourceDataSync",
        "ssm:DeleteResourceDataSync"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:resource-data-sync/InspectorResourceDataSync-do-not-delete"
      ]
    },
    {
      "Sid" : "ManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
      ]
    },
    {
      "Sid" : "LambdaCodeVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
```

```
        "codeguru-security:GetAccountConfiguration",
        "codeguru-security:GetFindings",
        "codeguru-security:GetScan",
        "codeguru-security:ListFindings",
        "codeguru-security:BatchGetFindings",
        "codeguru-security:DeleteScansByCategory"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CodeGuruCodeVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListAttachedRolePolicies",
        "iam:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "codeguru-security.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "Ec2DeepInspection",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:GetParameters",
        "ssm:DeleteParameter"
      ],
```

```
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/inspector-aws/service/inspector-linux-application-
paths"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowManagementOfServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/inspector2/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListServiceLinkedChannels",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToRunInvokeCisSpecificDocuments",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AmazonInspector2-InvokeInspectorSsmPluginCIS"
      ]
    },
    {
      "Sid" : "AllowToRunCisCommandsToSpecificResources",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToPutCloudwatchMetricData",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Inspector2"
        }
      }
    },
    {
      "Sid" : "AllowListAccessToECSAndEKS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListClusters",
        "ecs:ListTasks",
```

```
        "eks:ListClusters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowAccessToECSTasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTasks"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowInspectorEnablementForAwsOrgPolicy",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:Enable",
        "inspector2:Disable",
        "inspector2:EnableDelegatedAdminAccount",
        "inspector2:AssociateMember"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowInspectorServiceDelegatedAdminFromAwsOrg",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
```

```
          "organizations:ServicePrincipal" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonInspector2ThirdPartyServiceRolePolicy

Descrição: Concede permissões para que o Amazon Inspector realize ações em seu nome para a verificação de recursos em várias nuvens.

`AmazonInspector2ThirdPartyServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 26 de junho de 2026, 15:27 UTC
- Horário editado: 26 de junho de 2026, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ThirdPartyServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MultiCloudResourceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Search"
      ],
      "Resource" : "arn:aws:resource-explorer-2:*:*:view/ServiceViewForInspector*/
service-view"
    },
    {
      "Sid" : "MultiCloudStreamingAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateStreamingAccessForService",
        "resource-explorer-2:ListStreamingAccessForServices",
        "resource-explorer-2:DeleteStreamingAccessForService"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MultiCloudSsmAssociationWrite",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:StartAssociationsOnce"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-InstallDistributorPackageOnAzure*",
```

```
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "MultiCloudSsmAssociationDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation"
      ],
      "Resource" : "arn:aws:ssm:*:*:association/*"
    },
    {
      "Sid" : "MultiCloudSsmAssociationList",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListAssociations",
        "ssm:DescribeAssociationExecutions",
        "ssm:DescribeAssociationExecutionTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MultiCloudSsmGetDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AmazonInspector2-*",
        "arn:aws:ssm:*:*:document/AWS-InstallDistributorPackageOnAzure*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MultiCloudSsmAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:GetAutomationExecution",
        "ssm:DescribeAutomationExecutions",
```

```
        "ssm:DescribeAutomationStepExecutions",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-InstallDistributorPackageOnAzure*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ]
    },
    {
      "Sid" : "MultiCloudCloudConnectorManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateCloudConnector",
        "ssm:UpdateCloudConnector",
        "ssm:DeleteCloudConnector",
        "ssm:GetCloudConnector",
        "ssm:ListCloudConnectors",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:cloud-connector/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MultiCloudSsmPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/Inspector2SSMFederationRole*",
        "arn:aws:iam::*:role/Inspector2SSMDispatchRole*",
        "arn:aws:iam::*:role/Inspector2SSMAssumeRole*",
        "arn:aws:iam::*:role/Inspector2VmScannerRole*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "MultiCloudIamGetRole",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*:role/Inspector2SSMFederationRole*",
        "arn:aws:iam::*:role/Inspector2SSMDispatchRole*",
        "arn:aws:iam::*:role/Inspector2SSMAssumeRole*",
        "arn:aws:iam::*:role/Inspector2VmScannerRole*"
      ]
    },
    {
      "Sid" : "MultiCloudConfigSLRecWrite",
      "Effect" : "Allow",
      "Action" : [
        "config:PutThirdPartyServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MultiCloudConfigConnectorRead",
      "Effect" : "Allow",
      "Action" : [
        "config:ListConfigurationRecorders",
        "config:GetConnector"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MultiCloudConfigMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowGetWebIdentityToken",
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "sts:IdentityTokenAudience" : "false"
        },
        "ForAnyValue:StringLike" : {
          "sts:IdentityTokenAudience" : [
            "api://AzureADTokenExchange"
          ]
        }
      }
    },
    {
      "Sid" : "MultiCloudSsmSLRCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonInspectorFullAccess

Descrição: fornece acesso total ao Amazon Inspector.

`AmazonInspectorFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonInspectorFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 07 de outubro de 2015, 17:08 UTC
- Hora da edição: 21 de dezembro de 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorFullAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:*",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "sns:ListTopics",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "inspector.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/
AWSServiceRoleForAmazonInspector",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "inspector.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonInspectorReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon Inspector.

`AmazonInspectorReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonInspectorReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 07 de outubro de 2015, 17:08 UTC
- Hora da edição: 01 de outubro de 2019, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "sns:ListTopics",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonInspectorServiceRolePolicy

Descrição: Concede ao Amazon Inspector o acesso Serviços da AWS necessário para realizar avaliações de segurança

`AmazonInspectorServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 21 de novembro de 2017, 15:48 UTC
- Hora da edição: 11 de setembro de 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "directconnect:DescribeTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:GetTransitGatewayRouteTablePropagations",
```

```
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonKendraFullAccess

Descrição: Fornece acesso total ao Amazon Kendra por meio do. Console de gerenciamento da AWS

`AmazonKendraFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonKendraFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 03 de dezembro de 2019, 16:15 UTC
- Hora da edição: 03 de dezembro de 2019, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "kendra.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonKendra-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kendra:*",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonKendraReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon Kendra por meio do. Console de gerenciamento da AWS

`AmazonKendraReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonKendraReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 03 de dezembro de 2019, 16:13 UTC
- Hora da edição: 27 de maio de 2021, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "kendra:Describe*",
        "kendra:List*",
        "kendra:Query",
        "kendra:GetQuerySuggestions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonKeyspacesFullAccess

Descrição: fornece acesso total ao Amazon Keyspaces

`AmazonKeyspacesFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonKeyspacesFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de abril de 2020, 17:06 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CassandraFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchAlarmsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
```

```
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KeyspacesReplicationServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
replication.cassandra.amazonaws.com/AWSServiceRoleForKeyspacesReplication",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "replication.cassandra.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KeyspacesCDCServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra-
streams.amazonaws.com/AWSServiceRoleForAmazonKeyspacesCDC",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra-streams.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2VpcReadAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonKeyspacesReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon Keyspaces

`AmazonKeyspacesReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonKeyspacesReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de abril de 2020, 17:07 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:ListStreams",
        "cassandra:GetStream",
        "cassandra:GetShardIterator",
        "cassandra:GetRecords"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonKeyspacesReadOnlyAccess_v2

Descrição: Forneça acesso somente para leitura ao Amazon Keyspaces e AWS serviços relacionados.

`AmazonKeyspacesReadOnlyAccess_v2` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonKeyspacesReadOnlyAccess_v2` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 12 de setembro de 2023, 17:01 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "cassandra:Select",
        "cassandra:ListStreams",
        "cassandra:GetStream",
        "cassandra:GetShardIterator",
        "cassandra:GetRecords"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonKinesisAnalyticsFullAccess

Descrição: Fornece acesso total ao Amazon Kinesis Analytics por meio do Console de gerenciamento da AWS.

`AmazonKinesisAnalyticsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonKinesisAnalyticsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 21 de setembro de 2016, 19:01 UTC
- Hora da edição: 21 de setembro de 2016, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kinesisanalytics:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:CreateStream",
```

```
        "kinesis:DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLogEvents",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicyVersions",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/kinesis-analytics*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonKinesisAnalyticsReadOnly

Descrição: Fornece acesso somente para leitura ao Amazon Kinesis Analytics por meio do. Console de gerenciamento da AWS

`AmazonKinesisAnalyticsReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonKinesisAnalyticsReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 21 de setembro de 2016, 18:16 UTC
- Hora da edição: 21 de setembro de 2016, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisanalytics:Describe*",
        "kinesisanalytics:Get*",
        "kinesisanalytics:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLogEvents",
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicyVersions",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonKinesisFirehoseFullAccess

Descrição: fornece acesso total a todos os fluxos de entrega do Amazon Kinesis Firehose.

`AmazonKinesisFirehoseFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonKinesisFirehoseFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 07 de outubro de 2015, 18:45 UTC
- Hora da edição: 07 de outubro de 2015, 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "firehose:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonKinesisFirehoseReadOnlyAccess

Descrição: fornece acesso somente leitura a todos os fluxos de entrega do Amazon Kinesis Firehose.

`AmazonKinesisFirehoseReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonKinesisFirehoseReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 07 de outubro de 2015, 18:43 UTC
- Hora da edição: 07 de outubro de 2015, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "firehose:Describe*",
        "firehose:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonKinesisFullAccess

Descrição: Fornece acesso total a todos os streams por meio do Console de gerenciamento da AWS.

`AmazonKinesisFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonKinesisFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kinesis:*",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonKinesisReadOnlyAccess

Descrição: Fornece acesso somente para leitura a todos os fluxos por meio do Console de gerenciamento da AWS.

`AmazonKinesisReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonKinesisReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:Get*",
        "kinesis:List*",
        "kinesis:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonKinesisVideoStreamsFullAccess

Descrição: Fornece acesso total ao Amazon Kinesis Video Streams por meio do. Console de gerenciamento da AWS

`AmazonKinesisVideoStreamsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonKinesisVideoStreamsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2017, 23:27 UTC
- Hora da edição: 01 de dezembro de 2017, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kinesisvideo:*",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonKinesisVideoStreamsReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao AWS Kinesis Video Streams por meio do. Console de gerenciamento da AWS

`AmazonKinesisVideoStreamsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonKinesisVideoStreamsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2017, 23:14 UTC
- Hora da edição: 01 de dezembro de 2017, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:Describe*",
        "kinesisvideo:Get*",
        "kinesisvideo:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonLaunchWizard_Acesso total

Descrição: Acesso total ao assistente de AWS inicialização e outros serviços necessários.

`AmazonLaunchWizard_Fullaccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonLaunchWizard_Fullaccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de agosto de 2020, 17:47 UTC
- Hora da edição: 22 de fevereiro de 2023, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess`

Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:List*",
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets",
        "route53:GetChange",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:List*",
        "cloudwatch:Get*",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateVpc",
        "ec2:CreateKeyPair",
```

```
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AllocateHosts",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateVolume",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVolumeAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVolume",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteKeyPair",
        "ec2:DeleteNatGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DeleteSnapshot",
        "ec2:AssociateRouteTable",
        "ec2:AssociateVpcCidrBlock",
        "ec2:DeleteNetworkAcl",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DetachNetworkInterface",
        "ec2:DisassociateAddress",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:GetLaunchTemplateData",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:GetConsoleOutput",
        "ec2:GetPasswordData",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:ModifyInstancePlacement",
        "ec2:DeletePlacementGroup",
        "ec2:CreatePlacementGroup",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "ds:AddIpRoutes",
        "ds:CreateComputer",
        "ds:CreateMicrosoftAD",
        "ds:DeleteDirectory",
        "servicecatalog:AssociateProductWithPortfolio",
        "cloudformation:GetTemplateSummary",
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:Get*",
        "cloudformation:ListStacks",
        "cloudformation:SignalResource",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/LaunchWizard*/*",
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:role/service-role/AmazonLambdaRoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream",
        "logs:DescribeLog*",
        "logs:PutLogEvents",
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "sns:ListSubscriptionsByTopic",
        "sns:Publish",
        "ssm:DeleteDocument",
        "ssm:DeleteParameter*",
        "ssm:DescribeDocument*",
        "ssm:GetDocument",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/LaunchWizard*",
        "arn:aws:sns:*:*:*",
```

```
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*",
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunShellScript"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogStream",
        "logs:GetLogEvents",
        "logs:PutLogEvents",
        "ssm:AddTagsToResource",
        "ssm:DescribeDocument",
        "ssm:GetDocument",
```

```
        "ssm:ListTagsForResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "ds:Describe*",
        "ds:ListAuthorizedApplications",
        "ec2:Describe*",
        "ec2:Get*",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:List*",
        "logs:CreateLogGroup",
        "logs:GetLogDelivery",
        "logs:GetLogRecord",
        "logs:ListLogDeliveries",
        "resource-groups:Get*",
        "resource-groups:List*",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListServiceQuotas",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "ssm:CreateDocument",
        "ssm:DescribeAutomation*",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetCommandInvocation",
```

```
        "ssm:GetParameter*",
        "ssm:GetConnectionStatus",
        "ssm:ListCommand*",
        "ssm:ListDocument*",
        "ssm:ListInstanceAssociations",
        "ssm:SendAutomationSignal",
        "tag:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLog*",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:List*",
        "cloudformation:Describe*"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "application-insights.amazonaws.com",
            "events.amazonaws.com",
            "autoscaling.amazonaws.com.cn",
            "events.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "launchwizard:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
        "sqs:GetQueueUrl",
        "sqs:AddPermission",
        "sqs:ListQueues",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "iam:GetInstanceProfile",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "route53:ListHostedZones",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::launchwizard*/*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
```

```
        "s3:DeleteBucket",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:LaunchWizard*",
        "arn:aws:s3:::launchwizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DescribeTable",
        "dynamodb:DeleteTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsMetadata"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:DeleteOpsMetadata",
      "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:UntagResource",
        "fsx:TagResource",
        "fsx:DeleteFileSystem",
        "fsx:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "LaunchWizard*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateFileSystem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:RequestTag/Name" : [
            "LaunchWizard*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:CreatePortfolio",
        "servicecatalog:DescribePortfolio",
        "servicecatalog:CreateConstraint",
        "servicecatalog:CreateProduct",
        "servicecatalog:AssociatePrincipalWithPortfolio",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:TagResource",
        "servicecatalog:UntagResource"
      ],
      "Resource" : [
        "arn:aws:servicecatalog:*:*:*/*",
        "arn:aws:catalog:*:*:*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:TagResource",
        "logs:UntagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:LaunchWizard*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonLaunchWizardFullAccessV2

Descrição: Acesso total ao assistente de AWS inicialização e outros serviços necessários.

`AmazonLaunchWizardFullAccessV2` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonLaunchWizardFullAccessV2` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de setembro de 2023, 17:14 UTC
- Horário editado: 18 de agosto de 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppInsightsActions0",
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupActions0",
      "Effect" : "Allow",
      "Action" : "resource-groups:List*",
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "Route53Actions0",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets",
        "route53:GetChange",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3Actions0",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsActions0",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:List*",
        "cloudwatch:Get*",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "Ec2Actions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateVpc",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2Actions1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AllocateHosts",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVolumeAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVolume",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteKeyPair",
        "ec2:DeleteNatGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DeleteSnapshot",
        "ec2:AssociateRouteTable",
        "ec2:AssociateVpcCidrBlock",
        "ec2:DeleteNetworkAcl",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DetachNetworkInterface",
        "ec2:DisassociateAddress",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:GetLaunchTemplateData",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVolume",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:ModifyInstancePlacement",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "ds:AddIpRoutes",
        "ds:CreateComputer",
        "ds:CreateMicrosoftAD",
        "ds:DeleteDirectory",
        "servicecatalog:AssociateProductWithPortfolio",
        "cloudformation:GetTemplateSummary",
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2InstanceActions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
```

```
        "ec2:GetPasswordData"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Sid" : "Ec2RunInstancesActions0",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2SecurityGroupActions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "Ec2TagActions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2VolumeActions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2NetworkInterfaceActions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2VpcEndpointActions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormationActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:Get*",
        "cloudformation:ListStacks",
        "cloudformation:SignalResource",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/LaunchWizard*/*",
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/*"
      ]
    },
```

```
    {
      "Sid" : "CloudFormationActions1",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:List*",
        "cloudformation:Describe*"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
    },
    {
      "Sid" : "CloudFormationActions2",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    },
    {
      "Sid" : "IamActions0",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
    {
      "Sid" : "IamActions1",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard",
        "arn:aws:iam::*:role/service-role/AmazonLambdaRoleForLaunchWizard",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "IamActions2",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "application-insights.amazonaws.com",
            "events.amazonaws.com",
            "autoscaling.amazonaws.com.cn",
            "events.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchWizardActions0",
      "Effect" : "Allow",
      "Action" : "launchwizard:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingActions0",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
```

```
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "sns:ListSubscriptionsByTopic",
        "sns:Publish",
        "ssm:DeleteDocument",
        "ssm:DeleteParameter*",
        "ssm:DescribeDocument*",
        "ssm:GetDocument",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/LaunchWizard*",
        "arn:aws:sns:*:*:*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Sid" : "SsmActions0",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunShellScript"
      ]
    },
    {
      "Sid" : "SsmActions1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Sid" : "SsmActions2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:DescribeDocument",
        "ssm:GetDocument",
        "ssm:ListTagsForResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Sid" : "SsmActions3",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "ds:Describe*",
        "ds:ListAuthorizedApplications",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeHosts",
        "ec2:DescribeTags",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribePlacementGroups",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:List*",
        "resource-groups:Get*",
        "resource-groups:List*",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListServiceQuotas",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "ssm:CreateDocument",
        "ssm:DescribeAutomation*",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetCommandInvocation",
        "ssm:GetParameter*",
        "ssm:GetConnectionStatus",
        "ssm:ListCommand*",
```

```
        "ssm:ListDocument*",
        "ssm:ListInstanceAssociations",
        "ssm:SendAutomationSignal",
        "tag:Get*",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SsmActions4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmActions6",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsMetadata",
        "ssm:DeleteOpsMetadata"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
    },
    {
      "Sid" : "SsmActions7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SqsActions0",
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
        "sqs:GetQueueUrl",
        "sqs:AddPermission",
        "sqs:ListQueues",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
    },
    {
      "Sid" : "CloudWatchActions1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "iam:GetInstanceProfile",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
    {
      "Sid" : "EfsActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "route53:ListHostedZones",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
```

```
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "backup:ListBackupPlans"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EfsCreateActions0",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EfsActions1",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Actions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::launchwizard*/*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
```

```
      ]
    },
    {
      "Sid" : "ElbActions0",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElbActions1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:RemoveTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2PlacementGroupActions0",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:placement-group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2LaunchTemplateActions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LambdaActions0",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
        "s3:DeleteBucket",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction",
        "lambda:TagResource",
        "lambda:UntagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:LaunchWizard*",
```

```
        "arn:aws:s3:::launchwizard*"
      ]
    },
    {
      "Sid" : "DynamodbActions0",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DescribeTable",
        "dynamodb:DeleteTable",
        "dynamodb:TagResource",
        "dynamodb:UntagResource"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
    },
    {
      "Sid" : "SecretsManagerActions0",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
    },
    {
      "Sid" : "SecretsManagerActions1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsActions0",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
```

```
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
    },
    {
      "Sid" : "FsxActions0",
      "Effect" : "Allow",
      "Action" : [
        "fsx:UntagResource",
        "fsx:TagResource",
        "fsx:DeleteFileSystem",
        "fsx:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "LaunchWizard*"
        }
      }
    },
    {
      "Sid" : "FsxSvmTagActions0",
      "Effect" : "Allow",
      "Action" : [
        "fsx:TagResource",
        "fsx:UntagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*",
        "arn:aws:fsx:*:*:volume/*/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Sid" : "FsxActions1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "fsx:CreateFileSystem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : [
            "LaunchWizard*"
          ]
        }
      }
    },
    {
      "Sid" : "FsxActions2",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceCatalogActions0",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:CreatePortfolio",
        "servicecatalog:DescribePortfolio",
        "servicecatalog:CreateConstraint",
        "servicecatalog:CreateProduct",
        "servicecatalog:AssociatePrincipalWithPortfolio",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:TagResource",
        "servicecatalog:UntagResource"
      ],
      "Resource" : [
        "arn:aws:servicecatalog:*:*:*/*",
        "arn:aws:catalog:*:*:*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LogsActions0",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DescribeLogStreams",
        "logs:UntagResource",
        "logs:TagResource",
        "logs:CreateLogGroup",
        "logs:DeleteLogStream",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogDelivery",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:ListLogDeliveries"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:LaunchWizard*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*:log-stream:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LogsActions1",
      "Effect" : "Allow",
      "Action" : "logs:DescribeLogGroups",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "FsxActions3",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        },
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Sid" : "FsxActions4",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "FsxActions5",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        },
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonLexChannelsAccess

Descrição: esta política permite que os clientes chamem o runtime do Lex a partir dos canais

`AmazonLexChannelsAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 13 de janeiro de 2021, 20:12 UTC
- Hora da edição: 13 de janeiro de 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:ListBots"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonLexFullAccess

Descrição: Fornece acesso total ao Amazon Lex por meio do Console de gerenciamento da AWS. Também fornece acesso para criar funções vinculadas ao serviço Lex e conceder permissões Lex para invocar um conjunto limitado de funções Lambda.

`AmazonLexFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonLexFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 11 de abril de 2017, 23:20 UTC
- Hora da edição: 16 de abril de 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexFullAccess`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexFullAccessStatement1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "lex:*",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech",
        "kendra:ListIndices",
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "logs:DescribeLogGroups",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "AmazonLexFullAccessStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonLex*",
      "Condition" : {
        "StringEquals" : {
          "lambda:Principal" : "lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement3",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement4",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : "lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement5",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement6",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement7",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement8",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "replication.lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement9",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ]
```

```
    },
    {
      "Sid" : "AmazonLexFullAccessStatement10",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lex.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement11",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lexv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement12",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "channels.lexv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement13",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lexv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonLexReadOnly

Descrição: fornece acesso somente leitura ao Amazon Lex.

`AmazonLexReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonLexReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de abril de 2017, 23:13 UTC
- Hora da edição: 13 de maio de 2024, 16:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexReadOnlyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "lex:GetBot",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "lex:GetBots",
        "lex:GetBotChannelAssociation",
        "lex:GetBotChannelAssociations",
```

```
        "lex:GetBotVersions",
        "lex:GetBuiltinIntent",
        "lex:GetBuiltinIntents",
        "lex:GetBuiltinSlotTypes",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetIntentVersions",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetSlotTypeVersions",
        "lex:GetUtterancesView",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
        "lex:DescribeBotRecommendation",
        "lex:DescribeBotReplica",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:ListBots",
        "lex:ListBotLocales",
        "lex:ListBotAliases",
        "lex:ListBotAliasReplicas",
        "lex:ListBotChannels",
        "lex:ListBotRecommendations",
        "lex:ListBotReplicas",
        "lex:ListBotVersions",
        "lex:ListBotVersionReplicas",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
        "lex:ListIntents",
        "lex:ListRecommendedIntents",
        "lex:ListSlots",
        "lex:ListSlotTypes",
        "lex:ListTagsForResource",
        "lex:SearchAssociatedTranscripts",
        "lex:ListCustomVocabularyItems"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonLexReplicationPolicy

Descrição: permite que o Amazon Lex replique recursos do Lex entre regiões em seu nome.

`AmazonLexReplicationPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 31 de janeiro de 2024, 23:29 UTC
- Horário editado: 24 de junho de 2025, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReplicationServicePolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "lex:BuildBotLocale",
        "lex:ListBotLocales",
        "lex:CreateBotAlias",
        "lex:UpdateBotAlias",
        "lex:DeleteBotAlias",
        "lex:DescribeBotAlias",
        "lex:CreateBotVersion",
        "lex:DeleteBotVersion",
        "lex:DescribeBotVersion",
        "lex:CreateExport",
        "lex:DescribeBot",
        "lex:UpdateExport",
        "lex:DescribeExport",
        "lex:DescribeBotLocale",
        "lex:DescribeIntent",
        "lex:ListIntents",
        "lex:DescribeSlotType",
        "lex:ListSlotTypes",
        "lex:DescribeSlot",
        "lex:ListSlots",
        "lex:DescribeCustomVocabulary",
        "lex:StartImport",
        "lex:DescribeImport",
        "lex:CreateBot",
        "lex:UpdateBot",
        "lex:DeleteBot",
        "lex:CreateBotLocale",
        "lex:UpdateBotLocale",
        "lex:DeleteBotLocale",
        "lex:CreateIntent",
```

```
        "lex:UpdateIntent",
        "lex:DeleteIntent",
        "lex:CreateSlotType",
        "lex:UpdateSlotType",
        "lex:DeleteSlotType",
        "lex:CreateSlot",
        "lex:UpdateSlot",
        "lex:DeleteSlot",
        "lex:CreateCustomVocabulary",
        "lex:UpdateCustomVocabulary",
        "lex:DeleteCustomVocabulary",
        "lex:DeleteBotChannel",
        "lex:ListTagsForResource",
        "lex:TagResource",
        "lex:UntagResource",
        "lex:CreateResourcePolicy",
        "lex:DeleteResourcePolicy",
        "lex:DescribeResourcePolicy",
        "lex:UpdateResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:lex:*:*:bot/*",
        "arn:aws:lex:*:*:bot-alias/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReplicationServicePolicyStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lex:CreateUploadUrl",
        "lex:ListBots"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "ReplicationServicePolicyStatement3",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lexv2.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonLexRunBotsOnly

Descrição: fornece acesso a APIs conversacionais do Amazon Lex.

`AmazonLexRunBotsOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonLexRunBotsOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de abril de 2017, 23:06 UTC
- Hora da edição: 18 de agosto de 2021, 0:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexRunBotsOnly`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lex:PostContent",
        "lex:PostText",
        "lex:PutSession",
        "lex:GetSession",
        "lex:DeleteSession",
        "lex:RecognizeText",
        "lex:RecognizeUtterance",
        "lex:StartConversation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonLexV2BotPolicy

Descrição: Fornece aos bots Lex V2 acesso para ligar para outros AWS serviços em seu nome.

`AmazonLexV2BotPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 13 de janeiro de 2021, 20:10 UTC
- Hora da edição: 13 de janeiro de 2021, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonLookoutEquipmentFullAccess

Descrição: fornece acesso total às operações do Amazon Lookout for Equipment

`AmazonLookoutEquipmentFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonLookoutEquipmentFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de abril de 2021, 15:52 UTC
- Hora da edição: 24 de novembro de 2021, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "lookoutequipment:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lookoutequipment.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "lookoutequipment.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonLookoutEquipmentReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon Lookout for Equipment

`AmazonLookoutEquipmentReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonLookoutEquipmentReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 05 de maio de 2021, 16:47 UTC
- Hora da edição: 10 de novembro de 2022, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutequipment:Describe*",
        "lookoutequipment:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonLookoutMetricsFullAccess

Descrição: concede acesso a todas as ações do Amazon Lookout for Metrics

`AmazonLookoutMetricsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonLookoutMetricsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 07 de maio de 2021, 0:43 UTC
- Hora da edição: 07 de maio de 2021, 0:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutmetrics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*LookoutMetrics*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lookoutmetrics.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonLookoutMetricsReadOnlyAccess

Descrição: concede acesso a todas as ações somente leitura do Amazon Lookout for Metrics

`AmazonLookoutMetricsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonLookoutMetricsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 07 de maio de 2021, 0:43 UTC
- Hora da edição: 04 de janeiro de 2022, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutmetrics:DescribeMetricSet",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:DescribeAnomalyDetectionExecutions",
        "lookoutmetrics:DescribeAlert",
```

```
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListTagsForResource",
        "lookoutmetrics:ListAnomalyGroupSummaries",
        "lookoutmetrics:ListAnomalyGroupTimeSeries",
        "lookoutmetrics:ListAnomalyGroupRelatedMetrics",
        "lookoutmetrics:GetAnomalyGroup",
        "lookoutmetrics:GetDataQualityMetrics",
        "lookoutmetrics:GetSampleData",
        "lookoutmetrics:GetFeedback"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonLookoutVisionConsoleFullAccess

Descrição: fornece acesso total ao Amazon Lookout for Vision e acesso limitado às dependências necessárias do serviço e do console.

`AmazonLookoutVisionConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonLookoutVisionConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de maio de 2021, 19:37 UTC
- Hora da edição: 11 de maio de 2021, 19:37 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketFirstUseSetupAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*"
```

```
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*/*"
    },
    {
      "Sid" : "LookoutVisionConsoleDatasetLabelingToolsAccess",
      "Effect" : "Allow",
      "Action" : [
        "groundtruthlabeling:RunGenerateManifestByCrawlingJob",
        "groundtruthlabeling:AssociatePatchToManifestJob",
        "groundtruthlabeling:DescribeConsoleJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleTagSelectorAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleKmsKeySelectorAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonLookoutVisionConsoleReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon Lookout for Vision e acesso limitado às dependências necessárias do serviço e do console.

`AmazonLookoutVisionConsoleReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonLookoutVisionConsoleReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 11 de maio de 2021, 19:32 UTC
- Hora da edição: 09 de dezembro de 2021, 2:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeProject",
        "lookoutvision:DescribeTrialDetection",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "lookoutvision:ListTrialDetections",
        "lookoutvision:ListModelPackagingJobs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3ObjectReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*/*"
    },
    {
      "Sid" : "LookoutVisionConsoleDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonLookoutVisionFullAccess

Descrição: fornece acesso total ao Amazon Lookout for Vision e acesso limitado às dependências necessárias.

`AmazonLookoutVisionFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonLookoutVisionFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de maio de 2021, 19:24 UTC
- Hora da edição: 11 de maio de 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonLookoutVisionReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon Lookout for Vision e acesso limitado às dependências necessárias.

`AmazonLookoutVisionReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonLookoutVisionReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de maio de 2021, 19:11 UTC
- Hora da edição: 09 de dezembro de 2021, 3:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
```

```
        "lookoutvision:DescribeProject",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "lookoutvision:ListModelPackagingJobs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMachineLearningBatchPredictionsAccess

Descrição: concede aos usuários permissão para solicitar previsões em lote do Amazon Machine Learning.

`AmazonMachineLearningBatchPredictionsAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMachineLearningBatchPredictionsAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de abril de 2015, 17:12 UTC
- Hora da edição: 09 de abril de 2015, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning:DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMachineLearningCreateOnlyAccess

Descrição: fornece acesso de criação para recursos de não previsão do Amazon Machine Learning.

`AmazonMachineLearningCreateOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMachineLearningCreateOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de abril de 2015, 17:18 UTC
- Hora da edição: 29 de junho de 2016, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning:Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMachineLearningFullAccess

Descrição: fornece acesso total a recursos do Amazon Machine Learning.

`AmazonMachineLearningFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMachineLearningFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de abril de 2015, 17:25 UTC
- Hora da edição: 09 de abril de 2015, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

Descrição: concede aos usuários permissão para criar e excluir o endpoint em tempo real para modelos do Amazon Machine Learning.

`AmazonMachineLearningManageRealTimeEndpointOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMachineLearningManageRealTimeEndpointOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de abril de 2015, 17:32 UTC
- Hora da edição: 09 de abril de 2015, 17:32 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateRealtimeEndpoint",
        "machinelearning:DeleteRealtimeEndpoint"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMachineLearningReadOnlyAccess

Descrição: fornece acesso somente leitura a recursos do Amazon Machine Learning.

`AmazonMachineLearningReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMachineLearningReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de abril de 2015, 17:40 UTC
- Hora da edição: 09 de abril de 2015, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMachineLearningRealTimePredictionOnlyAccess

Descrição: concede aos usuários permissão para solicitar previsões em tempo real do Amazon Machine Learning.

`AmazonMachineLearningRealTimePredictionOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMachineLearningRealTimePredictionOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de abril de 2015, 17:44 UTC
- Hora da edição: 09 de abril de 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Predict"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMachineLearningRoleforRedshiftDataSourceV3

Descrição: permite que o Machine Learning configure e use seus clusters do Redshift e locais de preparação do S3 para a fonte de dados do Redshift.

`AmazonMachineLearningRoleforRedshiftDataSourceV3` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMachineLearningRoleforRedshiftDataSourceV3` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 24 de junho de 2020, 18:00 UTC
- Hora da edição: 24 de junho de 2020, 18:00 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupIngress",
        "redshift:AuthorizeClusterSecurityGroupIngress",
        "redshift:CreateClusterSecurityGroup",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:ModifyCluster",
        "redshift:RevokeClusterSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:GetObject",
        "s3:PutObject"
      ],
```

```
      "Resource" : "arn:aws:s3:::amazon-machine-learning*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMacieFullAccess

Descrição: fornece acesso total ao Amazon Macie.

`AmazonMacieFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMacieFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de agosto de 2017, 14:54 UTC
- Hora da edição: 01 de julho de 2022, 0:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieFullAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "pricing:GetProducts",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMacieHandshakeRole

Descrição: concede permissão para criar o perfil vinculado ao serviço do Amazon Macie.

`AmazonMacieHandshakeRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMacieHandshakeRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 28 de junho de 2018, 15:46 UTC
- Hora da edição: 28 de junho de 2018, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMacieReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon Macie.

`AmazonMacieReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMacieReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de junho de 2023, 21:50 UTC
- Hora da edição: 15 de junho de 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMacieServiceRole

Descrição: concede ao Macie acesso somente leitura às dependências de recursos na sua conta para permitir a análise dos dados.

`AmazonMacieServiceRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMacieServiceRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 14 de agosto de 2017, 14:53 UTC
- Hora da edição: 14 de agosto de 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMacieServiceRolePolicy

Descrição: perfil vinculado ao serviço para Amazon Macie

`AmazonMacieServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 19 de junho de 2018, 22:17 UTC
- Hora da edição: 19 de maio de 2022, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccountAliases",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "s3:GetAccountPublicAccessBlock",
```

```
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/macie/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonManagedBlockchainConsoleFullAccess

Descrição: Fornece acesso total ao Amazon Managed Blockchain por meio do Console de gerenciamento da AWS

`AmazonManagedBlockchainConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonManagedBlockchainConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de abril de 2019, 21:23 UTC
- Hora da edição: 29 de abril de 2019, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonManagedBlockchainFullAccess

Descrição: fornece acesso total ao Amazon Managed Blockchain.

`AmazonManagedBlockchainFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonManagedBlockchainFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de abril de 2019, 21:39 UTC

- Hora da edição: 29 de abril de 2019, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonManagedBlockchainReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon Managed Blockchain.

`AmazonManagedBlockchainReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonManagedBlockchainReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário da criação: 30 de abril de 2019, 18:17 UTC
- Hora da edição: 30 de abril de 2019, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:Get*",
        "managedblockchain:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonManagedBlockchainServiceRolePolicy

Descrição: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo Amazon Managed Blockchain

`AmazonManagedBlockchainServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 17 de janeiro de 2020, 19:51 UTC
- Hora da edição: 17 de janeiro de 2020, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*:log-stream:*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMCSFullAccess

Descrição: fornece acesso total ao Amazon Managed Apache Cassandra Service

`AmazonMCSFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMCSFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 03 de dezembro de 2019, 13:45 UTC
- Hora da edição: 17 de abril de 2020, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMCSReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon Managed Apache Cassandra Service

`AmazonMCSReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMCSReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 03 de dezembro de 2019, 13:46 UTC
- Hora da edição: 17 de abril de 2020, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMechanicalTurkFullAccess

Descrição: fornece acesso total a todas as APIs no Amazon Mechanical Turk.

`AmazonMechanicalTurkFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMechanicalTurkFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de dezembro de 2015, 19:08 UTC
- Hora da edição: 11 de dezembro de 2015, 19:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mechanicalturk:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMechanicalTurkReadOnly

Descrição: fornece acesso a APIs somente leitura no Amazon Mechanical Turk.

`AmazonMechanicalTurkReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMechanicalTurkReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de dezembro de 2015, 19:08 UTC

- Hora da edição: 25 de setembro de 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mechanicalturk:Get*",
        "mechanicalturk:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMemoryDBFullAccess

Descrição: Fornece acesso total ao Amazon MemoryDB por meio do. Console de gerenciamento da AWS

`AmazonMemoryDBFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMemoryDBFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de outubro de 2021, 19:24 UTC
- Hora da edição: 08 de outubro de 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "memorydb:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/memorydb.amazonaws.com/
AWSServiceRoleForMemoryDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "memorydb.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMemoryDBReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon MemoryDB por meio do. Console de gerenciamento da AWS

`AmazonMemoryDBReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMemoryDBReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de outubro de 2021, 19:27 UTC
- Hora da edição: 08 de outubro de 2021, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "memorydb:Describe*",
        "memorydb:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMobileAnalyticsFinancialReportAccess

Descrição: fornece acesso somente leitura a todos os relatórios, incluindo dados financeiros de todos os recursos da aplicação.

`AmazonMobileAnalyticsFinancialReportAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMobileAnalyticsFinancialReportAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mobileanalytics:GetReports",
        "mobileanalytics:GetFinancialReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMobileAnalyticsFullAccess

Descrição: fornece acesso total a todos os recursos da aplicação.

`AmazonMobileAnalyticsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMobileAnalyticsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : "mobileanalytics:*",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMobileAnalyticsNon-financialReportAccess

Descrição: fornece acesso somente leitura a relatórios não financeiros para todos os recursos da aplicação.

`AmazonMobileAnalyticsNon-financialReportAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMobileAnalyticsNon-financialReportAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mobileanalytics:GetReports",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMobileAnalyticsWriteOnlyAccess

Descrição: fornece acesso somente gravação a dados de eventos put para todos os recursos da aplicação. (Recomendado para integração com SDK)

`AmazonMobileAnalyticsWriteOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMobileAnalyticsWriteOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mobileanalytics:PutEvents",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMonitronFullAccess

Descrição: fornece acesso total ao Amazon Monitron

`AmazonMonitronFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMonitronFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 02 de dezembro de 2020, 22:40 UTC
- Hora da edição: 08 de junho de 2022, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMonitronFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "monitron.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "monitron:*"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "monitron.*.amazonaws.com"
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "AWSSSOPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "ds:DescribeDirectories",
        "ds:DescribeTrusts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/monitron/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMQApiFullAccess

Descrição: Fornece acesso total ao AmazonMQ por meio do nosso. API/SDK

`AmazonMQApiFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMQApiFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de dezembro de 2018, 20:31 UTC
- Hora da edição: 04 de novembro de 2020, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mq:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "mq.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMQApiReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao AmazonMQ por meio de nosso. API/SDK

`AmazonMQApiReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMQApiReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de dezembro de 2018, 20:31 UTC
- Hora da edição: 18 de dezembro de 2018, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMQFullAccess

Descrição: Fornece acesso total ao AmazonMQ por meio do. Console de gerenciamento da AWS

`AmazonMQFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMQFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2017, 15:28 UTC
- Horário editado: 03 de setembro de 2026, 22:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQFullAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mq:*",
        "cloudformation:CreateStack",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/mq.amazonaws.com/
AWSServiceRoleForAmazonMQ",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "mq.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMQReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao AmazonMQ por meio do. Console de gerenciamento da AWS

`AmazonMQReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMQReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2017, 15:30 UTC
- Hora da edição: 28 de novembro de 2017, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMQServiceRolePolicy

Descrição: Política de função vinculada a serviços para o AWS Amazon MQ

`AmazonMQServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 04 de novembro de 2020, 16:07 UTC

- Hora da edição: 04 de novembro de 2020, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AMQManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AMQManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    }
  ]
```

```
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMSKConnectReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon MSK Connect

`AmazonMSKConnectReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMSKConnectReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 20 de setembro de 2021, 10:18 UTC
- Hora da edição: 18 de outubro de 2021, 9:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListWorkerConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeConnector"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:connector/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeCustomPlugin"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:custom-plugin/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeWorkerConfiguration"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:worker-configuration/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMSKFullAccess

Descrição: fornece acesso total ao Amazon MSK e outras permissões necessárias para suas dependências.

`AmazonMSKFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMSKFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de janeiro de 2019, 22:07 UTC
- Hora da edição: 18 de outubro de 2023, 11:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKFullAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:*",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcAttribute",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "S3:GetBucketPolicy",
        "firehose:TagDeliveryStream"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*",
        "arn:*:ec2:*:*:subnet/*",
        "arn:*:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
```

```
          "aws:RequestTag/ClusterArn" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "kafka.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/kafka.amazonaws.com/
AWSServiceRoleForKafka*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "kafka.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMSKReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon MSK

`AmazonMSKReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonMSKReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de janeiro de 2019, 22:28 UTC
- Hora da edição: 14 de janeiro de 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "kafka:Describe*",
        "kafka:List*",
        "kafka:Get*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMWAAServerlessServiceRolePolicy

Descrição: Fornece acesso ao Amazon Airflow Serverless Service para gerenciar a rede de seus fluxos de trabalho e acessar outros AWS serviços em seu nome

`AmazonMWAAServerlessServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 15 de novembro de 2025, 20:34 UTC
- Horário editado: 15 de novembro de 2025, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServerlessServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonMWAAServiceRolePolicy

Descrição: o perfil vinculado ao serviço usado pelo Amazon Managed Workflows for Apache Airflow.

`AmazonMWAAServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Hora da criação: 24 de novembro de 2020, 14:13 UTC
- Hora da edição: 17 de novembro de 2022, 0:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:airflow-*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "AmazonMWAAManaged"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonMWAAManaged" : false
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "AmazonMWAAManaged"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/MWAA"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonNimbleStudio-LaunchProfileWorker

Descrição: esta política concede acesso aos recursos necessários aos funcionários do Nimble Studio Launch Profile. Anexe essa política às instâncias do EC2 criadas pelo Nimble Studio Builder.

`AmazonNimbleStudio-LaunchProfileWorker` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonNimbleStudio-LaunchProfileWorker` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de abril de 2021, 4:47 UTC
- Hora da edição: 28 de abril de 2021, 4:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      },
      "Sid" : "GetLaunchProfileInitializationDependencies"
    }
  ],
  "Version" : "2012-10-17"
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonNimbleStudio-StudioAdmin

Descrição: esta política concede acesso aos recursos do Amazon Nimble Studio associados ao administrador do estúdio e aos recursos relacionados do estúdio em outros serviços. Anexe essa política à função de administrador associada ao seu estúdio.

`AmazonNimbleStudio-StudioAdmin` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonNimbleStudio-StudioAdmin` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de abril de 2021, 4:47 UTC
- Hora da edição: 22 de setembro de 2023, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Statement" : [
    {
      "Sid" : "StudioAdminFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:DeleteStreamingSession",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetEula",
        "nimble:AcceptEulas",
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListStreamingSessions",
        "nimble:GetStreamingImage",
        "nimble:ListStreamingImages",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents",
        "nimble:ListLaunchProfiles",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileMember",
        "nimble:ListLaunchProfileMembers",
        "nimble:PutLaunchProfileMembers",
        "nimble:UpdateLaunchProfileMember",
        "nimble:DeleteLaunchProfileMember"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonNimbleStudio-StudioUser

Descrição: esta política concede acesso aos recursos do Amazon Nimble Studio associados ao usuário do estúdio e aos recursos relacionados do estúdio em outros serviços. Anexe essa política à função de usuário associada ao seu estúdio.

`AmazonNimbleStudio-StudioUser` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonNimbleStudio-StudioUser` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de abril de 2021, 4:48 UTC
- Hora da edição: 22 de setembro de 2023, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "nimble:ListLaunchProfiles"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "nimble:requesterPrincipalId" : "${nimble:principalId}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListEulas",
```

```
        "nimble:ListEulaAcceptances",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "nimble:DeleteStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:ListStreamingSessions",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "nimble:ownedBy" : "${nimble:requesterPrincipalId}"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonODBAutonomousDatabaseAdmin

Descrição: Fornece acesso administrativo para gerenciar recursos do Banco de Dados Autônomo no Oracle Database@AWS.

`AmazonODBAutonomousDatabaseAdmin` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonODBAutonomousDatabaseAdmin` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de trabalho
- Horário de criação: 04 de setembro de 2026, 21:47 UTC
- Horário editado: 04 de setembro de 2026, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBAutonomousDatabaseAdmin`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:InitializeService",
        "odb:CreateAutonomousDatabase",
        "odb:GetAutonomousDatabase",
```

```
        "odb:UpdateAutonomousDatabase",
        "odb:DeleteAutonomousDatabase",
        "odb:ListAutonomousDatabases",
        "odb:ListAutonomousDatabaseClones",
        "odb:ListAutonomousDatabasePeers",
        "odb:StartAutonomousDatabase",
        "odb:StopAutonomousDatabase",
        "odb:RebootAutonomousDatabase",
        "odb:ShrinkAutonomousDatabase",
        "odb:SwitchoverAutonomousDatabase",
        "odb:FailoverAutonomousDatabase",
        "odb:RestoreAutonomousDatabase",
        "odb:CreateAutonomousDatabaseWallet",
        "odb:GetAutonomousDatabaseWalletDetails",
        "odb:CreateAutonomousDatabaseBackup",
        "odb:GetAutonomousDatabaseBackup",
        "odb:UpdateAutonomousDatabaseBackup",
        "odb:DeleteAutonomousDatabaseBackup",
        "odb:ListAutonomousDatabaseBackups",
        "odb:GetOdbNetwork",
        "odb:ListOdbNetworks",
        "odb:ListAutonomousDatabaseVersions",
        "odb:ListAutonomousDatabaseCharacterSets",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSLRActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : [
            "odb.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:TagResource",
        "odb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:autonomous-database/*",
        "arn:aws:odb:*:*:autonomous-database-backup/*"
      ]
    },
    {
      "Sid" : "AllowOutboundIntegrationActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:CreateOutboundIntegration",
        "odb:UpdateOutboundIntegration"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:autonomous-database/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonODBAutonomousVmClusterAdmin

Descrição: Fornece acesso administrativo para gerenciar recursos de cluster de VMs autônomas no Oracle Database@AWS

`AmazonODBAutonomousVmClusterAdmin` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonODBAutonomousVmClusterAdmin` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de trabalho
- Horário de criação: 07 de agosto de 2026, 01:12 UTC
- Horário editado: 04 de setembro de 2026, 21:17 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBAutonomousVmClusterAdmin`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:InitializeService",
```

```
        "odb:GetCloudExadataInfrastructure",
        "odb:GetCloudExadataInfrastructureUnallocatedResources",
        "odb:ListCloudExadataInfrastructures",
        "odb:CreateCloudAutonomousVmCluster",
        "odb:GetCloudAutonomousVmCluster",
        "odb:DeleteCloudAutonomousVmCluster",
        "odb:ListCloudAutonomousVmClusters",
        "odb:AssociateIamRoleToResource",
        "odb:DisassociateIamRoleFromResource",
        "odb:ListDbServers",
        "odb:GetOdbNetwork",
        "odb:ListOdbNetworks",
        "odb:ListAutonomousVirtualMachines",
        "odb:ListDbSystemShapes",
        "odb:ListGiVersions",
        "odb:ListSystemVersions",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:TagResource",
        "odb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:cloud-autonomous-vm-cluster/*"
      ]
    },
    {
      "Sid" : "AllowOutboundIntegrationActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:CreateOutboundIntegration",
```

```
        "odb:UpdateOutboundIntegration"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:cloud-autonomous-vm-cluster/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonODBExadataInfrastructureAdmin

Descrição: Fornece acesso administrativo para gerenciar os recursos do Exadata Infrastructure no Oracle Database@AWS

`AmazonODBExadataInfrastructureAdmin` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonODBExadataInfrastructureAdmin` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de trabalho
- Horário de criação: 07 de agosto de 2026, 01:12 UTC
- Horário editado: 04 de setembro de 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBExadataInfrastructureAdmin`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:InitializeService",
        "odb:CreateCloudExadataInfrastructure",
        "odb:GetCloudExadataInfrastructure",
        "odb:UpdateCloudExadataInfrastructure",
        "odb:GetCloudExadataInfrastructureUnallocatedResources",
        "odb:DeleteCloudExadataInfrastructure",
        "odb:ListCloudExadataInfrastructures",
        "odb:ListCloudVmClusters",
        "odb:ListCloudAutonomousVmClusters",
        "odb:GetDbServer",
        "odb:ListDbServers",
        "odb:ListDbSystemShapes",
        "odb:ListFlexComponents",
        "odb:PutResourcePolicy",
        "odb:GetResourcePolicy",
        "odb:DeleteResourcePolicy",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSLRActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "odb.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:TagResource",
        "odb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:cloud-exadata-infrastructure/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonODBExadataVmClusterAdmin

Descrição: Fornece acesso administrativo para gerenciar os recursos do cluster Exadata VM no Oracle Database@.AWS

`AmazonODBExadataVmClusterAdmin` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonODBExadataVmClusterAdmin` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de trabalho
- Horário de criação: 04 de setembro de 2026, 21:37 UTC
- Horário editado: 04 de setembro de 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBExadataVmClusterAdmin`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:InitializeService",
        "odb:GetCloudExadataInfrastructure",
        "odb:GetCloudExadataInfrastructureUnallocatedResources",
        "odb:ListCloudExadataInfrastructures",
```

```
        "odb:CreateCloudVmCluster",
        "odb:GetCloudVmCluster",
        "odb:DeleteCloudVmCluster",
        "odb:ListCloudVmClusters",
        "odb:AssociateIamRoleToResource",
        "odb:DisassociateIamRoleFromResource",
        "odb:CreateDbNode",
        "odb:GetDbNode",
        "odb:RebootDbNode",
        "odb:StartDbNode",
        "odb:StopDbNode",
        "odb:DeleteDbNode",
        "odb:ListDbNodes",
        "odb:GetDbServer",
        "odb:ListDbServers",
        "odb:GetOdbNetwork",
        "odb:ListOdbNetworks",
        "odb:ListDbSystemShapes",
        "odb:ListFlexComponents",
        "odb:ListGiVersions",
        "odb:ListSystemVersions",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:TagResource",
        "odb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:cloud-vm-cluster/*",
        "arn:aws:odb:*:*:db-node/*"
      ]
```

```
    },
    {
      "Sid" : "AllowOutboundIntegrationActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:CreateOutboundIntegration",
        "odb:UpdateOutboundIntegration"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:cloud-vm-cluster/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonODBExascaleStorageVaultAdmin

Descrição: Fornece acesso administrativo para gerenciar os recursos do cofre de armazenamento Exascale no Oracle Database@.AWS

`AmazonODBExascaleStorageVaultAdmin` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonODBExascaleStorageVaultAdmin` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de trabalho
- Horário de criação: 04 de setembro de 2026, 21:37 UTC

- Horário editado: 04 de setembro de 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBExascaleStorageVaultAdmin`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:InitializeService",
        "odb:CreateExascaleDbStorageVault",
        "odb:GetExascaleDbStorageVault",
        "odb:UpdateExascaleDbStorageVault",
        "odb:DeleteExascaleDbStorageVault",
        "odb:ListExascaleDbStorageVaults",
        "odb:ListExadbVmClusters",
        "odb:GetDbServer",
        "odb:ListDbServers",
        "odb:ListDbSystemShapes",
        "odb:ListFlexComponents",
        "odb:PutResourcePolicy",
        "odb:GetResourcePolicy",
        "odb:DeleteResourcePolicy",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowEC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSLRActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "odb.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:TagResource",
        "odb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:exascale-db-storage-vault/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonODBExascaleVmClusterAdmin

Descrição: Fornece acesso administrativo para gerenciar recursos de cluster de VM Exascale no Oracle Database@.AWS

`AmazonODBExascaleVmClusterAdmin` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonODBExascaleVmClusterAdmin` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de trabalho
- Horário de criação: 04 de setembro de 2026, 21:37 UTC
- Horário editado: 04 de setembro de 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBExascaleVmClusterAdmin`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:InitializeService",
        "odb:GetExascaleDbStorageVault",
        "odb:ListExascaleDbStorageVaults",
        "odb:CreateExadbVmCluster",
```

```
        "odb:GetExadbVmCluster",
        "odb:UpdateExadbVmCluster",
        "odb:DeleteExadbVmCluster",
        "odb:ListExadbVmClusters",
        "odb:AssociateVirtualMachinesToExadbVmCluster",
        "odb:DisassociateVirtualMachinesFromExadbVmCluster",
        "odb:AssociateIamRoleToResource",
        "odb:DisassociateIamRoleFromResource",
        "odb:CreateDbNode",
        "odb:GetDbNode",
        "odb:RebootDbNode",
        "odb:StartDbNode",
        "odb:StopDbNode",
        "odb:DeleteDbNode",
        "odb:ListDbNodes",
        "odb:GetDbServer",
        "odb:ListDbServers",
        "odb:GetOdbNetwork",
        "odb:ListOdbNetworks",
        "odb:ListDbSystemShapes",
        "odb:ListFlexComponents",
        "odb:ListGiVersions",
        "odb:ListGiMinorVersions",
        "odb:ListSystemVersions",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:TagResource",
        "odb:UntagResource"
      ],
      "Resource" : [
```

```
        "arn:aws:odb:*:*:exadb-vm-cluster/*",
        "arn:aws:odb:*:*:db-node/*"
      ]
    },
    {
      "Sid" : "AllowOutboundIntegrationActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:CreateOutboundIntegration",
        "odb:UpdateOutboundIntegration"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:exadb-vm-cluster/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonODBFullAccess

Descrição: Fornece acesso total aos recursos no Oracle Database@AWS

`AmazonODBFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonODBFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Tempo de criação: 23 de julho de 2026, 22:57 UTC

- Horário editado: 04 de setembro de 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonODBFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:InitializeService",
        "odb:CreateCloudExadataInfrastructure",
        "odb:GetCloudExadataInfrastructure",
        "odb:UpdateCloudExadataInfrastructure",
        "odb:GetCloudExadataInfrastructureUnallocatedResources",
        "odb:DeleteCloudExadataInfrastructure",
        "odb:ListCloudExadataInfrastructures",
        "odb:CreateCloudVmCluster",
        "odb:GetCloudVmCluster",
        "odb:DeleteCloudVmCluster",
        "odb:ListCloudVmClusters",
        "odb:CreateCloudAutonomousVmCluster",
        "odb:GetCloudAutonomousVmCluster",
        "odb:DeleteCloudAutonomousVmCluster",
        "odb:ListCloudAutonomousVmClusters",
        "odb:CreateExascaleDbStorageVault",
        "odb:GetExascaleDbStorageVault",
        "odb:UpdateExascaleDbStorageVault",
        "odb:DeleteExascaleDbStorageVault",
        "odb:ListExascaleDbStorageVaults",
        "odb:CreateExadbVmCluster",
```

```
        "odb:GetExadbVmCluster",
        "odb:UpdateExadbVmCluster",
        "odb:DeleteExadbVmCluster",
        "odb:ListExadbVmClusters",
        "odb:AssociateVirtualMachinesToExadbVmCluster",
        "odb:DisassociateVirtualMachinesFromExadbVmCluster",
        "odb:ListGiMinorVersions",
        "odb:CreateAutonomousDatabase",
        "odb:GetAutonomousDatabase",
        "odb:UpdateAutonomousDatabase",
        "odb:DeleteAutonomousDatabase",
        "odb:ListAutonomousDatabases",
        "odb:ListAutonomousDatabaseClones",
        "odb:ListAutonomousDatabasePeers",
        "odb:StartAutonomousDatabase",
        "odb:StopAutonomousDatabase",
        "odb:RebootAutonomousDatabase",
        "odb:ShrinkAutonomousDatabase",
        "odb:SwitchoverAutonomousDatabase",
        "odb:FailoverAutonomousDatabase",
        "odb:RestoreAutonomousDatabase",
        "odb:CreateAutonomousDatabaseWallet",
        "odb:GetAutonomousDatabaseWalletDetails",
        "odb:CreateAutonomousDatabaseBackup",
        "odb:GetAutonomousDatabaseBackup",
        "odb:UpdateAutonomousDatabaseBackup",
        "odb:DeleteAutonomousDatabaseBackup",
        "odb:ListAutonomousDatabaseBackups",
        "odb:CreateDbNode",
        "odb:GetDbNode",
        "odb:RebootDbNode",
        "odb:StartDbNode",
        "odb:StopDbNode",
        "odb:DeleteDbNode",
        "odb:ListDbNodes",
        "odb:GetDbServer",
        "odb:ListDbServers",
        "odb:AssociateIamRoleToResource",
        "odb:DisassociateIamRoleFromResource",
        "odb:CreateOdbNetwork",
        "odb:GetOdbNetwork",
        "odb:UpdateOdbNetwork",
        "odb:DeleteOdbNetwork",
        "odb:ListOdbNetworks",
```

```
        "odb:CreateOdbPeeringConnection",
        "odb:GetOdbPeeringConnection",
        "odb:UpdateOdbPeeringConnection",
        "odb:DeleteOdbPeeringConnection",
        "odb:ListOdbPeeringConnections",
        "odb:ListAutonomousVirtualMachines",
        "odb:ListDbSystemShapes",
        "odb:ListFlexComponents",
        "odb:ListGiVersions",
        "odb:ListSystemVersions",
        "odb:ListAutonomousDatabaseVersions",
        "odb:ListAutonomousDatabaseCharacterSets",
        "odb:PutResourcePolicy",
        "odb:GetResourcePolicy",
        "odb:DeleteResourcePolicy",
        "odb:CreateGrantShare",
        "odb:UpdateGrantShare",
        "odb:DeleteGrantShare",
        "odb:CreateOutboundIntegration",
        "odb:UpdateOutboundIntegration",
        "odb:TagResource",
        "odb:UntagResource",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOdbNetworkPeeringActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateOdbNetworkPeering",
        "ec2:ModifyOdbNetworkPeering",
        "ec2:DeleteOdbNetworkPeering"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowSLRActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "odb.amazonaws.com",
            "vpc-lattice.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonODBNetworkAdmin

Descrição: Fornece acesso administrativo aos recursos de rede do Oracle Database@AWS

`AmazonODBNetworkAdmin` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonODBNetworkAdmin` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de trabalho

- Horário de criação: 07 de agosto de 2026, 01:12 UTC
- Horário editado: 04 de setembro de 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AmazonODBNetworkAdmin`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:InitializeService",
        "odb:CreateOdbNetwork",
        "odb:GetOdbNetwork",
        "odb:UpdateOdbNetwork",
        "odb:DeleteOdbNetwork",
        "odb:ListOdbNetworks",
        "odb:CreateOdbPeeringConnection",
        "odb:GetOdbPeeringConnection",
        "odb:UpdateOdbPeeringConnection",
        "odb:DeleteOdbPeeringConnection",
        "odb:ListOdbPeeringConnections",
        "odb:PutResourcePolicy",
        "odb:GetResourcePolicy",
        "odb:DeleteResourcePolicy",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowEC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOdbNetworkPeeringActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateOdbNetworkPeering",
        "ec2:ModifyOdbNetworkPeering",
        "ec2:DeleteOdbNetworkPeering"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSLRActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "odb.amazonaws.com",
            "vpc-lattice.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "odb:TagResource",
        "odb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:odb:*:*:odb-network/*",
        "arn:aws:odb:*:*:odb-peering-connection/*"
```

```
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonODBReadOnlyAccess

Descrição: Fornece acesso somente para leitura aos recursos do Oracle Database@AWS

`AmazonODBReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonODBReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 07 de agosto de 2026, 01:12 UTC
- Horário editado: 04 de setembro de 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonODBReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowODBReads",
      "Effect" : "Allow",
      "Action" : [
        "odb:GetOciOnboardingStatus",
        "odb:GetCloudExadataInfrastructure",
        "odb:GetCloudExadataInfrastructureUnallocatedResources",
        "odb:ListCloudExadataInfrastructures",
        "odb:GetCloudVmCluster",
        "odb:ListCloudVmClusters",
        "odb:GetCloudAutonomousVmCluster",
        "odb:ListCloudAutonomousVmClusters",
        "odb:GetExascaleDbStorageVault",
        "odb:ListExascaleDbStorageVaults",
        "odb:GetExadbVmCluster",
        "odb:ListExadbVmClusters",
        "odb:ListGiMinorVersions",
        "odb:GetAutonomousDatabase",
        "odb:ListAutonomousDatabases",
        "odb:ListAutonomousDatabaseClones",
        "odb:ListAutonomousDatabasePeers",
        "odb:GetAutonomousDatabaseBackup",
        "odb:ListAutonomousDatabaseBackups",
        "odb:GetDbNode",
        "odb:ListDbNodes",
        "odb:GetDbServer",
        "odb:ListDbServers",
        "odb:GetOdbNetwork",
        "odb:ListOdbNetworks",
        "odb:GetOdbPeeringConnection",
        "odb:ListOdbPeeringConnections",
        "odb:ListAutonomousVirtualMachines",
        "odb:ListDbSystemShapes",
        "odb:ListFlexComponents",
        "odb:ListGiVersions",
        "odb:ListSystemVersions",
        "odb:ListAutonomousDatabaseVersions",
        "odb:ListAutonomousDatabaseCharacterSets",
```

```
        "odb:GetResourcePolicy",
        "odb:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2Reads",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonODBServiceRolePolicy

Descrição: Permite que o Oracle Database@AWS gerencie AWS recursos em seu nome.

`AmazonODBServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Horário de criação: 13 de novembro de 2024, 18:21 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonODBServiceRolePolicy`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/ODB"
          ]
        }
      }
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "NM",
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EB1",
      "Effect" : "Allow",
      "Action" : [
        "events:ActivateEventSource",
        "events:DescribeEventSource"
      ],
      "Resource" : "arn:aws:events:*:*:event-source/aws.partner/odb*"
    },
    {
      "Sid" : "EB2",
      "Effect" : "Allow",
      "Action" : [
        "events:CreateEventBus",
        "events:DescribeEventBus"
      ],
      "Resource" : "arn:aws:events:*:*:event-bus/aws.partner/odb*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonOmicsFullAccess

Descrição: fornece acesso total ao Amazon Omics e outros Serviços da AWS necessários. Essa política permite que o usuário visualize e aceite convites de compartilhamento de RAM para acessar recursos fora do usuário. Conta da AWS

`AmazonOmicsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonOmicsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de fevereiro de 2023, 0:59 UTC
- Hora da edição: 24 de fevereiro de 2023, 0:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "omics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "omics.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "omics.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonOmicsReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon Omics

`AmazonOmicsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonOmicsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2022, 4:17 UTC

- Hora da edição: 29 de novembro de 2022, 4:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "omics:Get*",
        "omics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonOneEnterpriseFullAccess

Descrição: esta política concede permissões administrativas que permitem acesso a todos os recursos e operações do Amazon One Enterprise.

`AmazonOneEnterpriseFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonOneEnterpriseFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2023, 4:58 UTC
- Hora da edição: 28 de novembro de 2023, 4:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FullAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonOneEnterpriseInstallerAccess

Descrição: esta política concede permissões limitadas de leitura e gravação que permitem a instalação e ativação de dispositivos.

`AmazonOneEnterpriseInstallerAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonOneEnterpriseInstallerAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2023, 5:00 UTC
- Hora da edição: 28 de novembro de 2023, 5:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
```

```
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonOneEnterpriseReadOnlyAccess

Descrição: esta política concede permissões somente leitura para acesso a todos os recursos e operações do Amazon One Enterprise.

`AmazonOneEnterpriseReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonOneEnterpriseReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2023, 4:59 UTC
- Hora da edição: 28 de novembro de 2023, 4:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:Get*",
        "one:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonOpenSearchDashboardsServiceRolePolicy

Descrição: Fornece acesso ao Amazon OpenSearch Dashboards Service para acessar outros AWS serviços, como CloudWatch em seu nome

`AmazonOpenSearchDashboardsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 22 de dezembro de 2023, 19:38 UTC
- Hora da edição: 22 de dezembro de 2023, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonOpenSearchDashboardsServiceRoleAllowedActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AOSD"
        }
      }
    }
  ]
```

```
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonOpenSearchDirectQueryGlueCreateAccess

Descrição: permite que o OpenSearch DirectQuery Service acesse as APIs do AWS Glue para criar recursos em seu nome.

`AmazonOpenSearchDirectQueryGlueCreateAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonOpenSearchDirectQueryGlueCreateAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 6 de maio de 2024, 12:24 UTC
- Hora da edição: 06 de maio de 2024, 12:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchDirectQueryGlueCreateAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AmazonOpenSearchDirectQueryGlueCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:BatchCreatePartition"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonOpenSearchIngestionFullAccess

Descrição: permite que o Amazon OpenSearch Ingestion acesse outros AWS serviços em seu nome.

`AmazonOpenSearchIngestionFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonOpenSearchIngestionFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de abril de 2023, 18:11 UTC
- Hora da edição: 26 de abril de 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:CreatePipeline",
        "osis:UpdatePipeline",
        "osis:DeletePipeline",
        "osis:StartPipeline",
        "osis:StopPipeline",
        "osis:ListPipelines",
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:ValidatePipeline",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:TagResource",
        "osis:UntagResource",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/osis.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchIngestionService",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "osis.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonOpenSearchIngestionReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon OpenSearch Ingestion Service

`AmazonOpenSearchIngestionReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonOpenSearchIngestionReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de abril de 2023, 18:09 UTC
- Hora da edição: 26 de abril de 2023, 18:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonOpenSearchIngestionServiceRolePolicy

Descrição: permite que o Amazon OpenSearch Ingestion Service acesse outros AWS serviços em seu nome.

`AmazonOpenSearchIngestionServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 18 de novembro de 2022, 16:49 UTC
- Horário editado: 28 de agosto de 2025, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OSISManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OSISManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/OSIS"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonOpenSearchServerlessServiceRolePolicy

Descrição: Permita que o Amazon OpenSearch Serverless acesse outros AWS serviços, como CloudWatch APIs, em seu nome.

`AmazonOpenSearchServerlessServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 24 de novembro de 2022, 19:50 UTC
- Hora da edição: 25 de julho de 2024, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAOSSCloudwatchMetrics",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AOSS"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonOpenSearchServiceCognitoAccess

Descrição: fornece acesso ao serviço de configuração do Amazon Cognito.

`AmazonOpenSearchServiceCognitoAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonOpenSearchServiceCognitoAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 2 de setembro de 2021, 6:31 UTC
- Hora da edição: 20 de dezembro de 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:AdminInitiateAuth",
        "cognito-idp:AdminUserGlobalSignOut",
        "cognito-idp:ListUserPoolClients",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:UpdateIdentityPool",
        "cognito-identity:GetIdentityPoolRoles"
```

```
      ],
      "Resource" : [
        "arn:aws:cognito-identity:*:*:identitypool/*",
        "arn:aws:cognito-idp:*:*:userpool/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com",
            "cognito-identity-us-gov.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "cognito-identity:SetIdentityPoolRoles",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonOpenSearchServiceFullAccess

Descrição: Fornece acesso total ao serviço de configuração do Amazon OpenSearch Service.

`AmazonOpenSearchServiceFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonOpenSearchServiceFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 8 de setembro de 2021, 5:33 UTC
- Hora da edição: 8 de setembro de 2021, 5:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonOpenSearchServiceReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao serviço de configuração do Amazon OpenSearch Service.

`AmazonOpenSearchServiceReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonOpenSearchServiceReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 8 de setembro de 2021, 5:38 UTC
- Hora da edição: 8 de setembro de 2021, 5:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "es:Describe*",
        "es:List*",
        "es:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonOpenSearchServiceRolePolicy

Descrição: Permita que o Amazon OpenSearch Service acesse outros AWS serviços, como APIs de rede do EC2, em seu nome.

`AmazonOpenSearchServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 26 de agosto de 2021, 9:27 UTC
- Horário editado: 27 de março de 2025, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973145",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973144",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
```

```
    {
      "Sid" : "Stmt1480452973165",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973149",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973150",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973154",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973164",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "Stmt1480452973174",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973184",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973194",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973195",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973196",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "Stmt1480452973197",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/ES",
            "AWS/OpenSearch"
          ]
        }
      }
    },
    {
      "Sid" : "Stmt1480452973198",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973199",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973200",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
```

```
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973201",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973202",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sso:PutApplicationAccessScope",
      "Resource" : "arn:aws:sso::*:application/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonPersonalizeFullAccess

Descrição: Fornece acesso total ao Amazon Personalize por meio do SDK Console de gerenciamento da AWS e. Também fornece acesso selecionado a serviços relacionados (por exemplo, S3 CloudWatch).

`AmazonPersonalizeFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonPersonalizeFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 04 de dezembro de 2018, 22:24 UTC
- Hora da edição: 30 de maio de 2019, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "personalize:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*Personalize*",
        "arn:aws:s3:::*personalize*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "personalize.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonPollyFullAccess

Descrição: concede acesso total a serviços e recursos do Amazon Polly.

`AmazonPollyFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonPollyFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de novembro de 2016, 18:59 UTC
- Hora da edição: 30 de novembro de 2016, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "polly:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonPollyReadOnlyAccess

Descrição: concede acesso somente leitura a recursos do Amazon Polly.

`AmazonPollyReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonPollyReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de novembro de 2016, 18:59 UTC
- Horário editado: 01 de abril de 2026, 08:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech",
        "polly:StartSpeechSynthesisStream"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonPrometheusConsoleFullAccess

Descrição: Concede acesso total aos recursos do AWS Managed Prometheus no console AWS

`AmazonPrometheusConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonPrometheusConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de dezembro de 2020, 18:11 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagValues",
        "tag:GetTagKeys"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace",
        "aps:DescribeWorkspace",
        "aps:UpdateWorkspaceAlias",
```

```
        "aps:DeleteWorkspace",
        "aps:ListWorkspaces",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeRuleGroupsNamespace",
        "aps:CreateAlertManagerDefinition",
        "aps:CreateRuleGroupsNamespace",
        "aps:DeleteAlertManagerDefinition",
        "aps:DeleteRuleGroupsNamespace",
        "aps:ListRuleGroupsNamespaces",
        "aps:PutAlertManagerDefinition",
        "aps:PutRuleGroupsNamespace",
        "aps:TagResource",
        "aps:UntagResource",
        "aps:CreateLoggingConfiguration",
        "aps:UpdateLoggingConfiguration",
        "aps:DeleteLoggingConfiguration",
        "aps:DescribeLoggingConfiguration",
        "aps:UpdateWorkspaceConfiguration",
        "aps:DescribeWorkspaceConfiguration",
        "aps:CreateQueryLoggingConfiguration",
        "aps:UpdateQueryLoggingConfiguration",
        "aps:DeleteQueryLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonPrometheusFullAccess

Descrição: Concede acesso total aos recursos do AWS Managed Prometheus

`AmazonPrometheusFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonPrometheusFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de dezembro de 2020, 18:10 UTC
- Hora da edição: 26 de novembro de 2023, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllPrometheusActions",
      "Effect" : "Allow",
      "Action" : [
        "aps:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "aps.amazonaws.com"
          ]
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "scraper.aps.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonPrometheusQueryAccess

Descrição: Concede acesso para executar consultas em recursos AWS gerenciados do Prometheus

`AmazonPrometheusQueryAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonPrometheusQueryAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 19 de dezembro de 2020, 1:02 UTC
- Hora da edição: 19 de dezembro de 2020, 1:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonPrometheusRemoteWriteAccess

Descrição: Concede acesso somente de gravação aos espaços de trabalho AWS gerenciados do Prometheus

`AmazonPrometheusRemoteWriteAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonPrometheusRemoteWriteAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 19 de dezembro de 2020, 1:04 UTC
- Hora da edição: 19 de dezembro de 2020, 1:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:RemoteWrite"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonPrometheusScraperServiceRolePolicy

Descrição: Fornece acesso aos AWS recursos gerenciados ou usados pelo Amazon Managed Service for Prometheus Collector

`AmazonPrometheusScraperServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 26 de novembro de 2023, 14:19 UTC
- Horário editado: 17 de julho de 2026, 08:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScraperServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper*"
    },
    {
      "Sid" : "NetworkDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ENIManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AMPAgentlessScraper"
          ]
        }
      }
    },
    {
      "Sid" : "TagManagement",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "Null" : {
          "aws:RequestTag/AMPAgentlessScraper" : "false"
        }
      }
    },
    {
      "Sid" : "ENIUpdating",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AMPAgentlessScraper" : "false"
        }
      }
    },
    {
      "Sid" : "EKSAccess",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "DeleteEKSAccessEntry",
      "Effect" : "Allow",
      "Action" : "eks:DeleteAccessEntry",
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        },
        "ArnLike" : {
          "eks:principalArn" : "arn:aws:iam::*:role/aws-service-role/
scraper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScraper*"
```

```
        }
      }
    },
    {
      "Sid" : "APSWriting",
      "Effect" : "Allow",
      "Action" : "aps:RemoteWrite",
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchMetricsWriting",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "arn:aws:cloudwatch:*:*:dataset/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonQDeveloperAccess

Descrição: : fornece acesso de desenvolvedor para permitir interações com o Amazon Q

`AmazonQDeveloperAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonQDeveloperAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 9 de julho de 2024, 8:35 UTC
- Horário editado: 20 de maio de 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQDeveloperAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAmazonQDeveloperAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest",
        "q:StartTroubleshootingAnalysis",
        "q:StartTroubleshootingResolutionExplanation",
        "q:GetTroubleshootingResults",
        "q:UpdateTroubleshootingCommandResult",
        "q:GetIdentityMetaData",
```

```
        "q:GenerateCodeFromCommands",
        "q:UsePlugin"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCloudControlReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetResource",
        "cloudformation:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "AllowQArtifactsAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:CreateArtifact",
        "q:GetArtifact",
        "q:GetArtifactActionResult",
        "q:PerformArtifactAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonQFullAccess

Descrição: fornece acesso total para permitir interações com o Amazon Q.

`AmazonQFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonQFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2023, 16:00 UTC
- Horário editado: 20 de maio de 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQFullAccess`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAmazonQFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
```

```
        "q:PassRequest",
        "q:StartTroubleshootingAnalysis",
        "q:GetTroubleshootingResults",
        "q:StartTroubleshootingResolutionExplanation",
        "q:UpdateTroubleshootingCommandResult",
        "q:GetIdentityMetadata",
        "q:CreateAssignment",
        "q:DeleteAssignment",
        "q:GenerateCodeFromCommands",
        "q:CreatePlugin",
        "q:UpdatePlugin",
        "q:DeletePlugin",
        "q:GetPlugin",
        "q:UsePlugin",
        "q:ListPlugins",
        "q:ListPluginProviders",
        "q:ListTagsForResource",
        "q:UntagResource",
        "q:TagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowQArtifactsAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:CreateArtifact",
        "q:GetArtifact",
        "q:GetArtifactActionResult",
        "q:PerformArtifactAction"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCloudControlReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetResource",
        "cloudformation:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "AllowPassRoleToAmazonQ",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "q.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonQLDBConsoleFullAccess

Descrição: Fornece acesso total ao Amazon QLDB por meio do. Console de gerenciamento da AWS

`AmazonQLDBConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonQLDBConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 05 de setembro de 2019, 18:24 UTC
- Hora da edição: 04 de novembro de 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:CreateLedger",
        "qldb:UpdateLedger",
        "qldb:UpdateLedgerPermissionsMode",
        "qldb:DeleteLedger",
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ExportJournalToS3",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:CancelJournalKinesisStream",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:StreamJournalToKinesis",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
```

```
        "qldb:TagResource",
        "qldb:UntagResource",
        "qldb:ListTagsForResource",
        "qldb:SendCommand",
        "qldb:ExecuteStatement",
        "qldb:ShowCatalog",
        "qldb:InsertSampleData",
        "qldb:PartiQLCreateTable",
        "qldb:PartiQLCreateIndex",
        "qldb:PartiQLDropTable",
        "qldb:PartiQLDropIndex",
        "qldb:PartiQLUndropTable",
        "qldb:PartiQLDelete",
        "qldb:PartiQLInsert",
        "qldb:PartiQLUpdate",
        "qldb:PartiQLSelect",
        "qldb:PartiQLHistoryFunction",
        "qldb:PartiQLRedact"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dbqms:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:ListStreams",
        "kinesis:DescribeStream"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "qldb.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonQLDBFullAccess

Descrição: fornece acesso total ao Amazon QLDB via API do serviço.

`AmazonQLDBFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonQLDBFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 05 de setembro de 2019, 18:23 UTC
- Hora da edição: 04 de novembro de 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBFullAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:CreateLedger",
        "qldb:UpdateLedger",
        "qldb:UpdateLedgerPermissionsMode",
        "qldb:DeleteLedger",
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ExportJournalToS3",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:CancelJournalKinesisStream",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:StreamJournalToKinesis",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:GetBlock",
        "qldb:TagResource",
        "qldb:UntagResource",
        "qldb:ListTagsForResource",
        "qldb:SendCommand",
        "qldb:PartiQLCreateTable",
        "qldb:PartiQLCreateIndex",
        "qldb:PartiQLDropTable",
        "qldb:PartiQLDropIndex",
        "qldb:PartiQLUndropTable",
        "qldb:PartiQLDelete",
        "qldb:PartiQLInsert",
        "qldb:PartiQLUpdate",
        "qldb:PartiQLSelect",
        "qldb:PartiQLHistoryFunction",
        "qldb:PartiQLRedact"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "qldb.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonQLDBReadOnly

Descrição: fornece acesso somente leitura ao Amazon QLDB.

`AmazonQLDBReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonQLDBReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 05 de setembro de 2019, 18:19 UTC
- Hora da edição: 02 de julho de 2021, 2:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBReadOnly`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRDSBetaServiceRolePolicy

Descrição: permite que o Amazon RDS gerencie AWS recursos em seu nome.

`AmazonRDSBetaServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 02 de maio de 2018, 19:41 UTC
- Hora da edição: 7 de agosto de 2024, 0:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
```

```
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
```

```
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB",
            "AWS/Neptune",
            "AWS/RDS",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*"
      ],
```

```
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRDSCustomInstanceProfileRolePolicy

Descrição: permite que o Amazon RDS Custom execute várias ações de automação e tarefas de gerenciamento de banco de dados por meio de um perfil de instância do EC2.

`AmazonRDSCustomInstanceProfileRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRDSCustomInstanceProfileRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de fevereiro de 2024, 17:42 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ssmAgentPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "ssmAgentPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetManifest",
        "ssm:PutConfigurePackageResult"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssmAgentPermission4",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:OpenControlChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission5",
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "createEc2SnapshotPermission1",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createEc2SnapshotPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createEc2SnapshotPermission3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
```

```
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createTagForEc2SnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateSnapshot",
            "CreateSnapshots"
          ]
        }
      }
    },
    {
      "Sid" : "rdsCustomS3ObjectPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:putObject",
        "s3:getObject",
        "s3:getObjectVersion",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "rdsCustomS3BucketPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucketVersions",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "readSecretsFromCpPermission",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createSecretsOnDpPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : "custom-oracle-rac"
        }
      }
    },
    {
      "Sid" : "publishCwMetricsPermission",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "rdscustom/rds-custom-sqlserver-agent",
            "RDSCustomForOracle/Agent"
          ]
        }
      }
    },
    {
      "Sid" : "putEventsToEventBusPermission",
      "Effect" : "Allow",
      "Action" : "events:PutEvents",
      "Resource" : "arn:aws:events:*:*:event-bus/default"
    },
    {
      "Sid" : "cwlUploadPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutRetentionPolicy",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:rds-custom-instance-*"
    },
    {
      "Sid" : "sendMessageToSqsQueuePermission",
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : "custom-sqlserver"
        }
      }
    },
    {
      "Sid" : "managePrivateIpOnEniPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : "custom-oracle-rac"
        }
      }
    },
    {
      "Sid" : "kmsPermissionWithSecret",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
```

```
          "kms:EncryptionContext:SecretARN" : [
            "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
            "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "kmsPermissionWithS3",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-rds-custom-
*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRDSCustomPreviewServiceRolePolicy

Descrição: política de perfil de serviço de pré-visualização do Amazon RDS Custom

`AmazonRDSCustomPreviewServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 08 de outubro de 2021, 21:44 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
```

```
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
```

```
    },
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccKeyPair2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface1",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "eccNetworkInterface2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "eccNetworkInterface3",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "eccCreateTag2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateKeyPair",
            "RunInstances",
            "CreateNetworkInterface",
            "CreateVolume",
            "CreateSnapshots",
            "CopySnapshot",
            "AllocateAddress"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "eccVolume2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume4snapshot1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "eccSnapshotCopySource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/snap-*"
    },
    {
      "Sid" : "eccSnapshotCopyDestination",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/${*}"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWSRDSCustom*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds-preview.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:EnableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds-preview.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager2",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RestoreSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager3",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "sqs1",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:TagQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "sqs2",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:DeleteQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle"
          ]
        }
      }
```

```
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRDSCustomServiceRolePolicy

Descrição: permite que o Amazon RDS Custom gerencie AWS recursos em seu nome.

`AmazonRDSCustomServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 08 de outubro de 2021, 21:39 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

Versão da política

Versão da política: v19 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "rdscrc",
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
```

```
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "eccModifyInstanceAttribute1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ],
          "ec2:Attribute" : "InstanceType"
        }
      }
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccKeyPair2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface1",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "eccNetworkInterface2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "eccNetworkInterface3",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "eccCreateTag2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateKeyPair",
            "RunInstances",
            "CreateNetworkInterface",
            "CreateVolume",
            "CreateSnapshot",
            "CreateSnapshots",
            "CopySnapshot",
            "AllocateAddress",
            "CopyImage"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "eccVolume2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume4snapshot1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "eccSnapshot4",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshotCopySource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/snap-*"
    },
    {
      "Sid" : "eccSnapshotCopyDestination",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/${*}"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "eccAmi1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ]
    },
    {
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWSRDSCustom*",
        "arn:aws:iam::*:role/service-role/AWSRDSCustom*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
```

```
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:EnableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
```

```
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager2",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
```

```
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RestoreSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager3",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "sqs1",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:TagQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-sqlserver",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "sqs2",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:DeleteQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRDSDataFullAccess

Descrição: permite acesso total ao uso das APIs de dados do RDS, APIs de armazenamento secreto para credenciais do banco de dados do RDS e APIs de gerenciamento de consultas do console de banco de dados para executar instruções SQL em clusters do Aurora Sem Servidor na Conta da AWS.

`AmazonRDSDataFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRDSDataFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 20 de novembro de 2018, 21:29 UTC
- Hora da edição: 20 de novembro de 2019, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSDataFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerDbCredentialsAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutResourcePolicy",
```

```
        "secretsmanager:PutSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-db-credentials/*"
    },
    {
      "Sid" : "RDSDataServiceAccess",
      "Effect" : "Allow",
      "Action" : [
        "dbqms:CreateFavoriteQuery",
        "dbqms:DescribeFavoriteQueries",
        "dbqms:UpdateFavoriteQuery",
        "dbqms:DeleteFavoriteQueries",
        "dbqms:GetQueryString",
        "dbqms:CreateQueryHistory",
        "dbqms:DescribeQueryHistory",
        "dbqms:UpdateQueryHistory",
        "dbqms:DeleteQueryHistory",
        "rds-data:ExecuteSql",
        "rds-data:ExecuteStatement",
        "rds-data:BatchExecuteStatement",
        "rds-data:BeginTransaction",
        "rds-data:CommitTransaction",
        "rds-data:RollbackTransaction",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:GetRandomPassword",
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRDSDirectoryServiceAccess

Descrição: permite que o RDS acesse o Directory Service Managed AD em nome do cliente para instâncias de banco de dados SQL Server associadas ao domínio.

`AmazonRDSDirectoryServiceAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRDSDirectoryServiceAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 26 de fevereiro de 2016, 2:02 UTC
- Hora da edição: 15 de maio de 2019, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRDSEnhancedMonitoringRole

Descrição: fornece acesso ao Cloudwatch para monitoramento aprimorado do RDS

`AmazonRDSEnhancedMonitoringRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRDSEnhancedMonitoringRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 11 de novembro de 2015, 19:58 UTC
- Hora da edição: 11 de novembro de 2015, 19:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:RDS*"
      ]
    },
    {
      "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:RDS*:log-stream:*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRDSFullAccess

Descrição: Fornece acesso total ao Amazon RDS por meio do Console de gerenciamento da AWS.

`AmazonRDSFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRDSFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 17 de agosto de 2023, 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSFullAccess`

Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
```

```
        "application-autoscaling:RegisterScalableTarget",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:GetCoipPoolUsage",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "outposts:GetOutpostInstanceTypes",
        "devops-guru:GetResourceCollection"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "pi:*",
      "Resource" : [
        "arn:aws:pi:*:*:metrics/rds/*",
        "arn:aws:pi:*:*:perf-reports/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "iam:AWSServiceName" : [
            "rds.amazonaws.com",
            "rds.application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "devops-guru:SearchInsights",
        "devops-guru:ListAnomaliesForInsight"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "devops-guru:ServiceNames" : [
            "RDS"
          ]
        },
        "Null" : {
          "devops-guru:ServiceNames" : "false"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRDSPerformanceInsightsFullAccess

Descrição: Fornece acesso total ao RDS Performance Insights por meio do Console de gerenciamento da AWS

`AmazonRDSPerformanceInsightsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRDSPerformanceInsightsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de agosto de 2023, 23:41 UTC
- Horário editado: 23 de julho de 2026, 00:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSPerformanceInsightsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics"
      ],
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
```

```
    {
      "Sid" : "AmazonRDSPerformanceInsightsAnalisysReportFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:CreatePerformanceAnalysisReport",
        "pi:GetPerformanceAnalysisReport",
        "pi:ListPerformanceAnalysisReportRecommendations",
        "pi:ListPerformanceAnalysisReports",
        "pi:DeletePerformanceAnalysisReport"
      ],
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsTaggingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:TagResource",
        "pi:UntagResource",
        "pi:ListTagsForResource"
      ],
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
    },
    {
      "Sid" : "AmazonRDSDescribeInstanceAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:ListTagsForResource",
        "rds:DescribeDBShardGroups"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:shard-group:*"
      ]
    },
    {
      "Sid" : "AmazonCloudWatchReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRDSPerformanceInsightsReadOnly

Descrição: Read-Only política para o RDS Performance Insights

`AmazonRDSPerformanceInsightsReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRDSPerformanceInsightsReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 05 de abril de 2022, 0:02 UTC
- Horário editado: 22 de julho de 2026, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSDescribeDBInstances",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Sid" : "AmazonRDSDescribeDBClusters",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBClusters",
      "Resource" : "arn:aws:rds:*:*:cluster:*"
    },
    {
      "Sid" : "AmazonRDSDescribeDBShardGroups",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBShardGroups",
      "Resource" : "arn:aws:rds:*:*:shard-group:*"
    },
    {
      "Sid" : "AmazonRDSListTagsForResource",
      "Effect" : "Allow",
      "Action" : "rds:ListTagsForResource",
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:shard-group:*",
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsDescribeDimensionKeys",
      "Effect" : "Allow",
      "Action" : "pi:DescribeDimensionKeys",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetDimensionKeyDetails",
      "Effect" : "Allow",
      "Action" : "pi:GetDimensionKeyDetails",
```

```
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetadata",
      "Effect" : "Allow",
      "Action" : "pi:GetResourceMetadata",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetrics",
      "Effect" : "Allow",
      "Action" : "pi:GetResourceMetrics",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceDimensions",
      "Effect" : "Allow",
      "Action" : "pi:ListAvailableResourceDimensions",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceMetrics",
      "Effect" : "Allow",
      "Action" : "pi:ListAvailableResourceMetrics",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetPerformanceAnalysisReport",
      "Effect" : "Allow",
      "Action" : "pi:GetPerformanceAnalysisReport",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" :
 "AmazonRDSPerformanceInsightsListPerformanceAnalysisReportRecommendations",
      "Effect" : "Allow",
      "Action" : "pi:ListPerformanceAnalysisReportRecommendations",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListPerformanceAnalysisReports",
      "Effect" : "Allow",
      "Action" : "pi:ListPerformanceAnalysisReports",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
```

```
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListTagsForResource",
      "Effect" : "Allow",
      "Action" : "pi:ListTagsForResource",
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRDSPreviewServiceRolePolicy

Descrição: política de perfil de serviço de pré-visualização do Amazon RDS

`AmazonRDSPreviewServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 31 de maio de 2018, 18:02 UTC
- Hora da edição: 7 de agosto de 2024, 1:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB-Preview",
            "AWS/Neptune-Preview",
            "AWS/RDS-Preview",
            "AWS/Usage"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
```

```
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRDSReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon RDS por meio do Console de gerenciamento da AWS.

`AmazonRDSReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRDSReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 14 de abril de 2023, 12:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:Describe*",
        "rds:ListTagsForResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "devops-guru:GetResourceCollection"
      ],
      "Resource" : "*"
    },
    {
      "Action" : [
        "devops-guru:SearchInsights",
        "devops-guru:ListAnomaliesForInsight"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "devops-guru:ServiceNames" : [
            "RDS"
```

```
          ]
        },
        "Null" : {
          "devops-guru:ServiceNames" : "false"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRDSServiceRolePolicy

Descrição: permite que o Amazon RDS gerencie AWS recursos em seu nome.

`AmazonRDSServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 08 de janeiro de 2018, 18:17 UTC
- Hora da edição: 1º de julho de 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy`

Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CrossRegionCommunication",
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
```

```
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*"
      ]
    },
    {
      "Sid" : "CloudWatchStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    },
```

```
    {
      "Sid" : "Kinesis",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:CreateStream",
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream",
        "kinesis:SplitShard",
        "kinesis:MergeShards",
        "kinesis:DeleteStream",
        "kinesis:UpdateShardCount"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/aws-rds-das-*"
      ]
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB",
            "AWS/Neptune",
            "AWS/RDS",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPassword",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SecretsManagerSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
        }
      }
    },
    {
      "Sid" : "SecretsManagerTags",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRedshiftAllCommandsFullAccess

Descrição: esta política inclui permissões para executar comandos SQL para copiar, carregar, descarregar, consultar e analisar dados no Amazon Redshift. A política também concede permissões para executar instruções selecionadas para serviços relacionados, como Amazon S3, Amazon CloudWatch logs SageMaker, Amazon ou AWS Glue.

`AmazonRedshiftAllCommandsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRedshiftAllCommandsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 04 de novembro de 2021, 0:48 UTC
- Hora da edição: 25 de novembro de 2021, 2:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:InvokeEndpoint",
        "sagemaker:StopProcessingJob",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*redshift*",
        "arn:aws:sagemaker:*:*:training-job/*redshift*",
        "arn:aws:sagemaker:*:*:automl-job/*redshift*",
        "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
        "arn:aws:sagemaker:*:*:processing-job/*redshift*",
        "arn:aws:sagemaker:*:*:transform-job/*redshift*",
        "arn:aws:sagemaker:*:*:endpoint/*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/*redshift*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "SageMaker",
            "/aws/sagemaker/Endpoints",
            "/aws/sagemaker/ProcessingJobs",
            "/aws/sagemaker/TrainingJobs",
            "/aws/sagemaker/TransformJobs"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketCors",
        "s3:DeleteObject",
```

```
        "s3:AbortMultipartUpload",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::redshift-downloads",
        "arn:aws:s3:::redshift-downloads/*",
        "arn:aws:s3:::*redshift*",
        "arn:aws:s3:::*redshift*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/Redshift" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan",
        "dynamodb:DescribeTable",
        "dynamodb:Getitem"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/*redshift*",
        "arn:aws:dynamodb:*:*:table/*redshift*/index/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:ListInstances"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*redshift*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:ListInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "elasticmapreduce:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:*redshift*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*redshift*/*",
        "arn:aws:glue:*:*:catalog",
```

```
        "arn:aws:glue:*:*:database/*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "redshift.amazonaws.com",
            "glue.amazonaws.com",
            "sagemaker.amazonaws.com",
            "athena.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRedshiftDataFullAccess

Descrição: esta política fornece acesso total às APIs de dados do Amazon Redshift. Essa política também concede acesso a outros serviços necessários.

`AmazonRedshiftDataFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRedshiftDataFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de setembro de 2020, 19:23 UTC
- Hora da edição: 07 de abril de 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "DataAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
        }
      }
    },
    {
      "Sid" : "GetCredentialsForAPIUser",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbname:*/*",
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Sid" : "GetCredentialsWithFederatedIAMCredentials",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentialsWithIAM",
```

```
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*"
    },
    {
      "Sid" : "GetCredentialsForServerless",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetCredentials",
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/RedshiftDataFullAccess" : "*"
        }
      }
    },
    {
      "Sid" : "DenyCreateAPIUser",
      "Effect" : "Deny",
      "Action" : "redshift:CreateClusterUser",
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Sid" : "ServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/redshift-data.amazonaws.com/
AWSServiceRoleForRedshift",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "redshift-data.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRedshiftFederatedAuthorization

Descrição: Essa é uma política fácil de usar para executar consultas com a Autorização Federada do Amazon Redshift

`AmazonRedshiftFederatedAuthorization` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRedshiftFederatedAuthorization` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 22 de novembro de 2025, 00:04 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFederatedAuthorization`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRedshiftFederatedAuthorization",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
```

```
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetUserDefinedFunctions",
        "glue:CreateDatabase",
        "glue:CreateTable",
        "glue:DeleteDatabase",
        "glue:DeleteTable",
        "glue:UpdateCatalog",
        "glue:UpdateDatabase",
        "glue:UpdateTable",
        "glue:RenameTable",
        "glue:FederateAuthorization"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "glue:FederatedAuthorizationSource" : "Redshift"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftIdentityCenterSetContext",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRedshiftFullAccess

Descrição: Fornece acesso total ao Amazon Redshift por meio do Console de gerenciamento da AWS.

`AmazonRedshiftFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRedshiftFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 07 de julho de 2022, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "redshift:*",
        "redshift-serverless:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "sns:CreateTopic",
        "sns:Get*",
        "sns:List*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DisableAlarmActions",
        "tag:GetResources",
        "tag:UntagResources",
        "tag:GetTagValues",
        "tag:GetTagKeys",
        "tag:TagResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "redshift.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataAPIPermissions",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerListPermissions",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerCreateGetPermissions",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRedshiftQueryEditor

Descrição: fornece acesso total ao Editor de Consultas do Amazon Redshift e a consultas salvas via Console de gerenciamento da AWS.

`AmazonRedshiftQueryEditor` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRedshiftQueryEditor` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 04 de outubro de 2018, 22:50 UTC
- Hora da edição: 16 de fevereiro de 2021, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials",
        "redshift:ListSchemas",
        "redshift:ListTables",
        "redshift:ListDatabases",
        "redshift:ExecuteQuery",
        "redshift:FetchResults",
        "redshift:CancelQuery",
        "redshift:DescribeClusters",
        "redshift:DescribeQuery",
        "redshift:DescribeTable",
        "redshift:ViewQueriesFromConsole",
```

```
        "redshift:DescribeSavedQueries",
        "redshift:CreateSavedQuery",
        "redshift:DeleteSavedQueries",
        "redshift:ModifySavedQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataAPIPermissions",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "DataAPIIAMSessionPermissionsRestriction",
      "Action" : [
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:ListStatements"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerListPermissions",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SecretsManagerCreateGetPermissions",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/RedshiftQueryOwner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRedshiftQueryEditorV2FullAccess

Descrição: concede acesso total às operações e recursos do Editor de Consultas V2 do Amazon Redshift. Essa política também concede acesso a outros serviços necessários. Isso inclui permissões para listar os clusters do Amazon Redshift, ler chaves e aliases no AWS KMS e gerenciar os segredos do Query Editor V2 no Secrets Manager. AWS

`AmazonRedshiftQueryEditorV2FullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRedshiftQueryEditorV2FullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de setembro de 2021, 14:06 UTC
- Hora da edição: 21 de fevereiro de 2024, 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KeyManagementServicePermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*"
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2Permissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:*",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRedshiftQueryEditorV2NoSharing

Descrição: concede a capacidade de trabalhar com o Editor de Consultas V2 do Amazon Redshift sem compartilhar recursos. O principal concedido só pode ler, atualizar e excluir seus próprios recursos, mas não pode compartilhá-los. Essa política também concede acesso a outros serviços necessários. Isso inclui permissões para listar os clusters do Amazon Redshift e gerenciar os segredos do Query Editor V2 do principal no AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2NoSharing` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRedshiftQueryEditorV2NoSharing` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de setembro de 2021, 14:18 UTC
- Hora da edição: 21 de fevereiro de 2024, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
```

```
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
```

```
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRedshiftQueryEditorV2ReadSharing

Descrição: concede a capacidade de trabalhar com o Editor de Consultas V2 do Amazon Redshift com compartilhamento limitado de recursos. A entidade principal concedida pode ler, escrever e compartilhar seus próprios recursos. A entidade principal concedida pode ler os recursos compartilhados com sua equipe, mas não pode atualizá-los. Essa política também concede acesso a outros serviços necessários. Isso inclui permissões para listar os clusters do Amazon Redshift e gerenciar os segredos do Query Editor V2 do principal no AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2ReadSharing` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRedshiftQueryEditorV2ReadSharing` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de setembro de 2021, 14:22 UTC
- Hora da edição: 21 de fevereiro de 2024, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
```

```
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
```

```
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
```

```
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TeamReadAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:UntagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRedshiftQueryEditorV2ReadWriteSharing

Descrição: concede a capacidade de trabalhar com o Editor de Consultas V2 do Amazon Redshift com compartilhamento de recursos. A entidade principal concedida pode ler, escrever e compartilhar seus próprios recursos. A entidade principal concedida pode ler e atualizar os recursos compartilhados com sua equipe. Essa política também concede acesso a outros serviços necessários. Isso inclui permissões para listar os clusters do Amazon Redshift e gerenciar os segredos do Query Editor V2 do principal no AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2ReadWriteSharing` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRedshiftQueryEditorV2ReadWriteSharing` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de setembro de 2021, 14:25 UTC
- Hora da edição: 21 de fevereiro de 2024, 17:30 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
```

```
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
```

```
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TeamReadWriteAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
```

```
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:UntagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
```

```
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRedshiftReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon Redshift por meio do Console de gerenciamento da AWS.

`AmazonRedshiftReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRedshiftReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 8 de fevereiro de 2024, 0:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRedshiftReadOnlyAccess",
      "Action" : [
        "redshift:Describe*",
        "redshift:ListRecommendations",
        "redshift:ViewQueriesInConsole",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "sns:Get*",
        "sns:List*",
        "cloudwatch:Describe*",
        "cloudwatch:List*",
        "cloudwatch:Get*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRedshiftServiceLinkedRolePolicy

Descrição: Permite que o Amazon Redshift chame AWS serviços em seu nome

`AmazonRedshiftServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 18 de setembro de 2017, 19:19 UTC
- Horário editado: 19 de fevereiro de 2025, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2VpcPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PublicAccessCreateEip",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "PublicAccessReleaseEip",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/redshift/*"
      ]
    },
    {
      "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/redshift/*:log-stream:*"
      ]
    },
    {
      "Sid" : "CreateSecurityGroupWithTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
```

```
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:ModifySecurityGroupRules",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateTagsOnResources",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpc",
            "CreateSecurityGroup",
            "CreateSubnet",
            "CreateInternetGateway",
            "CreateRouteTable",
```

```
            "AllocateAddress"
          ]
        }
      }
    },
    {
      "Sid" : "VPCPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Redshift-Serverless",
            "AWS/Redshift"
          ]
        }
      }
    },
    {
      "Sid" : "SecretManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
```

```
        "secretsmanager:RotateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:redshift!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "redshift",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerRandomPassword",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IPV6Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "ServiceQuotasToCheckCustomerLimits",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:ec2/L-0263D0A3",
        "arn:aws:servicequotas:*:*:vpc/L-29B6F2EB"
      ]
    },
    {
      "Sid" : "DiscoverRedshiftCatalogs",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:GetCatalogs"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "Bool" : {
          "glue:EnabledForRedshiftAutoDiscovery" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LakeFormationGetMetadataAccessForFederatedCatalogs",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Bool" : {
          "lakeformation:EnabledOnlyForMetaDataAccess" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "glue.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRekognitionCustomLabelsFullAccess

Descrição: esta política especifica as permissões do Rekognition e do S3 exigidas pelo recurso Amazon Rekognition Custom Labels.

`AmazonRekognitionCustomLabelsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRekognitionCustomLabelsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de janeiro de 2020, 19:18 UTC
- Hora da edição: 16 de agosto de 2022, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*custom-labels*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:CreateProject",
        "rekognition:CreateProjectVersion",
        "rekognition:StartProjectVersion",
        "rekognition:StopProjectVersion",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DetectCustomLabels",
        "rekognition:DeleteProject",
        "rekognition:DeleteProjectVersion",
        "rekognition:TagResource",
        "rekognition:UntagResource",
        "rekognition:ListTagsForResource",
        "rekognition:CreateDataset",
        "rekognition:ListDatasetEntries",
        "rekognition:ListDatasetLabels",
        "rekognition:DescribeDataset",
        "rekognition:UpdateDatasetEntries",
        "rekognition:DistributeDatasetEntries",
        "rekognition:DeleteDataset",
        "rekognition:CopyProjectVersion",
        "rekognition:PutProjectPolicy",
        "rekognition:ListProjectPolicies",
        "rekognition:DeleteProjectPolicy"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRekognitionFullAccess

Descrição: acesso a todas as APIs do Amazon Rekognition

`AmazonRekognitionFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRekognitionFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de novembro de 2016, 14:40 UTC
- Hora da edição: 30 de novembro de 2016, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRekognitionReadOnlyAccess

Descrição: acesso a todas as APIs de leitura do Rekognition

`AmazonRekognitionReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRekognitionReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de novembro de 2016, 14:58 UTC
- Hora da edição: 08 de novembro de 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRekognitionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "rekognition:CompareFaces",
        "rekognition:DetectFaces",
        "rekognition:DetectLabels",
        "rekognition:ListCollections",
        "rekognition:ListFaces",
        "rekognition:SearchFaces",
        "rekognition:SearchFacesByImage",
        "rekognition:DetectText",
        "rekognition:GetCelebrityInfo",
        "rekognition:RecognizeCelebrities",
        "rekognition:DetectModerationLabels",
        "rekognition:GetLabelDetection",
        "rekognition:GetFaceDetection",
        "rekognition:GetContentModeration",
        "rekognition:GetPersonTracking",
        "rekognition:GetCelebrityRecognition",
        "rekognition:GetFaceSearch",
        "rekognition:GetTextDetection",
        "rekognition:GetSegmentDetection",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DetectCustomLabels",
        "rekognition:DetectProtectiveEquipment",
        "rekognition:ListTagsForResource",
```

```
        "rekognition:ListDatasetEntries",
        "rekognition:ListDatasetLabels",
        "rekognition:DescribeDataset",
        "rekognition:ListProjectPolicies",
        "rekognition:ListUsers",
        "rekognition:SearchUsers",
        "rekognition:SearchUsersByImage",
        "rekognition:GetMediaAnalysisJob",
        "rekognition:ListMediaAnalysisJobs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRekognitionServiceRole

Descrição: Permite que o Rekognition ligue para os AWS serviços em seu nome.

`AmazonRekognitionServiceRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRekognitionServiceRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 29 de novembro de 2017, 16:52 UTC
- Hora da edição: 29 de novembro de 2017, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:AmazonRekognition*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/AmazonRekognition*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:GetMedia"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53AutoNamingFullAccess

Descrição: fornece acesso total a todas as ações de nomenclatura automática do Route 53.

`AmazonRoute53AutoNamingFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53AutoNamingFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de janeiro de 2018, 18:40 UTC
- Hora da edição: 18 de janeiro de 2018, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "servicediscovery:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53AutoNamingReadOnlyAccess

Descrição: fornece acesso somente leitura a todas as ações de nomenclatura automática do Route 53.

`AmazonRoute53AutoNamingReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53AutoNamingReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de janeiro de 2018, 3:02 UTC
- Hora da edição: 18 de janeiro de 2018, 3:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:Get*",
        "servicediscovery:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53AutoNamingRegistrantAccess

Descrição: fornece acesso em nível de registrante às ações de nomenclatura automática do Route 53.

`AmazonRoute53AutoNamingRegistrantAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53AutoNamingRegistrantAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 12 de março de 2018, 22:33 UTC
- Hora da edição: 12 de março de 2018, 22:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
```

```
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53DomainsFullAccess

Descrição: fornece acesso total a todas as ações de domínios do Route53 e cria zona hospedada para permitir a criação de zonas hospedadas como parte dos registros de domínio.

`AmazonRoute53DomainsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53DomainsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC

- Hora da edição: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53DomainsReadOnlyAccess

Descrição: fornece acesso à lista e ações de domínios do Route53.

`AmazonRoute53DomainsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53DomainsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53FullAccess

Descrição: fornece acesso total ao Amazon Route 53 via Console de gerenciamento da AWS.

`AmazonRoute53FullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53FullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53FullAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:*",
        "route53domains:*",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistributionTenantByDomain",
        "cloudfront:GetConnectionGroup",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRegions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticbeanstalk:DescribeEnvironments",
        "es:ListDomainNames",
        "es:DescribeDomains",
        "lightsail:GetContainerServices",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : "arn:aws:apigateway:*::/domainnames"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53GlobalResolverFullAccess

Descrição: Fornece acesso total para recuperar, listar, criar, atualizar e excluir todos os recursos do Amazon Route 53 Global Resolver.

`AmazonRoute53GlobalResolverFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53GlobalResolverFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 09 de março de 2026, 20:27 UTC
- Horário editado: 09 de março de 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53GlobalResolverFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53GlobalResolverFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53globalresolver:AllowVendedLogDeliveryForResource",
        "route53globalresolver:AssociateHostedZone",
        "route53globalresolver:BatchCreateFirewallRule",
        "route53globalresolver:BatchDeleteFirewallRule",
        "route53globalresolver:BatchUpdateFirewallRule",
        "route53globalresolver:CreateAccessSource",
        "route53globalresolver:CreateAccessToken",
        "route53globalresolver:CreateDNSView",
        "route53globalresolver:CreateFirewallDomainList",
        "route53globalresolver:CreateFirewallRule",
        "route53globalresolver:CreateGlobalResolver",
        "route53globalresolver:DeleteAccessSource",
        "route53globalresolver:DeleteAccessToken",
        "route53globalresolver:DeleteDNSView",
        "route53globalresolver:DeleteFirewallDomainList",
        "route53globalresolver:DeleteFirewallRule",
        "route53globalresolver:DeleteGlobalResolver",
        "route53globalresolver:DisableDNSView",
        "route53globalresolver:DisassociateHostedZone",
        "route53globalresolver:EnableDNSView",
        "route53globalresolver:GetAccessSource",
        "route53globalresolver:GetAccessToken",
        "route53globalresolver:GetDNSView",
        "route53globalresolver:GetFirewallDomainList",
        "route53globalresolver:GetFirewallRule",
        "route53globalresolver:GetGlobalResolver",
        "route53globalresolver:GetHostedZoneAssociation",
        "route53globalresolver:GetManagedFirewallDomainList",
        "route53globalresolver:ImportFirewallDomains",
        "route53globalresolver:ListAccessSources",
        "route53globalresolver:ListAccessTokens",
        "route53globalresolver:ListDNSViews",
        "route53globalresolver:ListFirewallDomainLists",
        "route53globalresolver:ListFirewallDomains",
        "route53globalresolver:ListFirewallRules",
```

```
        "route53globalresolver:ListGlobalResolvers",
        "route53globalresolver:ListHostedZoneAssociations",
        "route53globalresolver:ListManagedFirewallDomainLists",
        "route53globalresolver:ListTagsForResource",
        "route53globalresolver:TagResource",
        "route53globalresolver:UntagResource",
        "route53globalresolver:UpdateAccessSource",
        "route53globalresolver:UpdateAccessToken",
        "route53globalresolver:UpdateDNSView",
        "route53globalresolver:UpdateFirewallDomains",
        "route53globalresolver:UpdateFirewallRule",
        "route53globalresolver:UpdateGlobalResolver",
        "route53globalresolver:UpdateHostedZoneAssociation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53GlobalResolverReadOnlyAccess

Descrição: Fornece acesso somente para leitura para recuperar e listar todos os recursos do Amazon Route 53 Global Resolver.

`AmazonRoute53GlobalResolverReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53GlobalResolverReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 09 de março de 2026, 20:27 UTC
- Horário editado: 09 de março de 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53GlobalResolverReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53GlobalResolverReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53globalresolver:GetAccessSource",
        "route53globalresolver:GetAccessToken",
        "route53globalresolver:GetDNSView",
        "route53globalresolver:GetFirewallDomainList",
        "route53globalresolver:GetFirewallRule",
        "route53globalresolver:GetGlobalResolver",
        "route53globalresolver:GetHostedZoneAssociation",
        "route53globalresolver:GetManagedFirewallDomainList",
        "route53globalresolver:ListAccessSources",
        "route53globalresolver:ListAccessTokens",
        "route53globalresolver:ListDNSViews",
        "route53globalresolver:ListFirewallDomainLists",
        "route53globalresolver:ListFirewallDomains",
        "route53globalresolver:ListFirewallRules",
        "route53globalresolver:ListGlobalResolvers",
        "route53globalresolver:ListHostedZoneAssociations",
```

```
        "route53globalresolver:ListManagedFirewallDomainLists"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53ProfilesFullAccess

Descrição: esta política concede acesso total aos recursos do Amazon Route 53 Profile.

`AmazonRoute53ProfilesFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53ProfilesFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de abril de 2024, 18:30 UTC
- Hora da edição: 27 de agosto de 2024, 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:AssociateProfile",
        "route53profiles:AssociateResourceToProfile",
        "route53profiles:CreateProfile",
        "route53profiles:DeleteProfile",
        "route53profiles:DisassociateProfile",
        "route53profiles:DisassociateResourceFromProfile",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfilePolicy",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53profiles:PutProfilePolicy",
        "route53profiles:TagResource",
        "route53profiles:UntagResource",
        "route53profiles:UpdateProfileResourceAssociation",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverRule",
        "ec2:DescribeVpcs",
        "route53:GetHostedZone"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53ProfilesReadOnlyAccess

Descrição: esta política concede acesso somente leitura aos recursos do Amazon Route 53 Profile.

`AmazonRoute53ProfilesReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53ProfilesReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de abril de 2024, 18:29 UTC
- Hora da edição: 27 de agosto de 2024, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfilePolicy",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53ReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon Route 53 via Console de gerenciamento da AWS.

`AmazonRoute53ReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53ReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 15 de novembro de 2016, 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53RecoveryClusterFullAccess

Descrição: fornece acesso total ao cluster de recuperação do Amazon Route 53

`AmazonRoute53RecoveryClusterFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53RecoveryClusterFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de agosto de 2021, 18:37 UTC
- Hora da edição: 18 de agosto de 2021, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53RecoveryClusterReadOnlyAccess

Descrição: fornece acesso somente leitura ao cluster de recuperação do Amazon Route 53

`AmazonRoute53RecoveryClusterReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53RecoveryClusterReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de agosto de 2021, 17:36 UTC
- Hora da edição: 01 de abril de 2022, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53RecoveryControlConfigFullAccess

Descrição: fornece acesso total à configuração do controle de recuperação do Amazon Route 53

`AmazonRoute53RecoveryControlConfigFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53RecoveryControlConfigFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de agosto de 2021, 17:48 UTC
- Hora da edição: 18 de agosto de 2021, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53RecoveryControlConfigReadOnlyAccess

Descrição: fornece acesso somente leitura à configuração do controle de recuperação do Amazon Route 53

`AmazonRoute53RecoveryControlConfigReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53RecoveryControlConfigReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de agosto de 2021, 18:01 UTC
- Hora da edição: 18 de outubro de 2023, 17:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeRoutingControlByName",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53RecoveryReadinessFullAccess

Descrição: fornece acesso total à prontidão de recuperação do Amazon Route 53

`AmazonRoute53RecoveryReadinessFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53RecoveryReadinessFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de agosto de 2021, 16:45 UTC
- Hora da edição: 18 de agosto de 2021, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53RecoveryReadinessReadOnlyAccess

Descrição: fornece acesso somente leitura à prontidão de recuperação do Amazon Route 53

`AmazonRoute53RecoveryReadinessReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53RecoveryReadinessReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de agosto de 2021, 18:11 UTC
- Hora da edição: 09 de novembro de 2021, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetReadinessCheckResourceStatus",
        "route53-recovery-readiness:GetReadinessCheckStatus",
```

```
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListCrossAccountAuthorizations",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53-recovery-readiness:ListRules",
        "route53-recovery-readiness:ListTagsForResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetArchitectureRecommendations",
        "route53-recovery-readiness:GetCellReadinessSummary"
      ],
      "Resource" : "arn:aws:route53-recovery-readiness::*:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53ResolverFullAccess

Descrição: política de acesso total para o Route 53 Resolver

`AmazonRoute53ResolverFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53ResolverFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de maio de 2019, 18:10 UTC
- Hora da edição: 5 de agosto de 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ResolverFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:*",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonRoute53ResolverReadOnlyAccess

Descrição: política de acesso somente leitura para o Route 53 Resolver

`AmazonRoute53ResolverReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonRoute53ResolverReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de maio de 2019, 18:11 UTC
- Hora da edição: 5 de agosto de 2024, 18:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ResolverReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonS3ExpressFullAccess

Descrição: Fornece acesso total a todos os buckets de diretório do S3.

`AmazonS3ExpressFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonS3ExpressFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de abril de 2026, 20:42 UTC
- Horário editado: 03 de abril de 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ExpressFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3ExpressFullAccess",
      "Effect" : "Allow",
      "Action" : "s3express:*",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonS3ExpressReadOnlyAccess

Descrição: Fornece acesso somente para leitura às operações do S3Express para buckets de diretório do S3.

`AmazonS3ExpressReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonS3ExpressReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de abril de 2026, 20:42 UTC
- Horário editado: 03 de abril de 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ExpressReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3ExpressReadOnlySessionObjectAccess",
      "Effect" : "Allow",
      "Action" : "s3express:CreateSession",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "s3express:SessionMode" : "ReadOnly"
        }
      }
    },
    {
      "Sid" : "S3ExpressReadOnlyControlPlaneAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonS3FilesClientFullAccess

Descrição: Fornece acesso ao cliente raiz a um sistema de arquivos do S3 Files.

`AmazonS3FilesClientFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonS3FilesClientFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 07 de abril de 2026, 12:57 UTC
- Horário editado: 07 de abril de 2026, 12:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesClientFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3files:ClientMount",
        "s3files:ClientWrite",
        "s3files:ClientRootAccess"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonS3FilesClientReadOnlyAccess

Descrição: Fornece acesso de cliente somente para leitura a um sistema de arquivos do S3 Files.

`AmazonS3FilesClientReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonS3FilesClientReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 07 de abril de 2026, 12:57 UTC
- Horário editado: 07 de abril de 2026, 12:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesClientReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3files:ClientMount"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonS3FilesClientReadWriteAccess

Descrição: Fornece acesso do cliente de leitura e gravação a um sistema de arquivos do S3 Files.

`AmazonS3FilesClientReadWriteAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonS3FilesClientReadWriteAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 07 de abril de 2026, 12:57 UTC
- Horário editado: 07 de abril de 2026, 12:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesClientReadWriteAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3files:ClientMount",
        "s3files:ClientWrite"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonS3FilesCSIDriverPolicy

Descrição: Fornece acesso de gerenciamento aos recursos do Amazon S3 Files

`AmazonS3FilesCSIDriverPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonS3FilesCSIDriverPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 07 de abril de 2026, 13:12 UTC

- Horário editado: 07 de abril de 2026, 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3FilesCSIDriverPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowList",
      "Effect" : "Allow",
      "Action" : [
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateAccessPoint",
      "Effect" : "Allow",
      "Action" : [
        "s3files:CreateAccessPoint"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
        }
      }
    },
```

```
    {
      "Sid" : "AllowTagNewAccessPoints",
      "Effect" : "Allow",
      "Action" : [
        "s3files:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3files:CreateAction" : "CreateAccessPoint"
        },
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
        }
      }
    },
    {
      "Sid" : "AllowDeleteAccessPoint",
      "Effect" : "Allow",
      "Action" : "s3files:DeleteAccessPoint",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/efs.csi.aws.com/cluster" : "false"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonS3FilesFullAccess

Descrição: Fornece acesso total a todos os arquivos do S3 por meio do Console de gerenciamento da AWS.

`AmazonS3FilesFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonS3FilesFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 07 de abril de 2026, 12:42 UTC
- Horário editado: 07 de abril de 2026, 12:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
      "Effect" : "Allow",
      "Action" : "s3files:*",
      "Resource" : "*"
    },
    {
      "Sid" : "EC2NetworkingPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketNotification",
        "s3:PutBucketNotification"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "EventBridgeManage",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "elasticfilesystem.amazonaws.com"
        }
      },
      "Resource" : [
        "arn:aws:events:*:*:rule/DO-NOT-DELETE-S3-Files*"
      ]
    },
    {
      "Sid" : "EventBridgeRead",
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:DescribeRule",
        "events:ListRules",
        "events:ListTargetsByRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/*"
      ]
    },
    {
      "Sid" : "IAMPassRoleForS3Files",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "elasticfilesystem.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonS3FilesReadOnlyAccess

Descrição: Fornece acesso somente para leitura a todos os arquivos do S3 por meio do Console de gerenciamento da AWS.

`AmazonS3FilesReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonS3FilesReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 07 de abril de 2026, 12:57 UTC
- Horário editado: 07 de abril de 2026, 12:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FilesReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3FilesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3files:Get*",
        "s3files:List*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonS3FullAccess

Descrição: Fornece acesso total a todos os buckets por meio do Console de gerenciamento da AWS.

`AmazonS3FullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonS3FullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 27 de setembro de 2021, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
        "s3-object-lambda:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonS3ObjectLambdaExecutionRolePolicy

Descrição: Fornece permissões às funções do AWS Lambda para interagir com o Amazon S3 Object Lambda. Também concede permissões ao Lambda para gravar em CloudWatch registros.

`AmazonS3ObjectLambdaExecutionRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonS3ObjectLambdaExecutionRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço

- Hora da criação: 18 de agosto de 2021, 10:07 UTC
- Hora da edição: 18 de agosto de 2021, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonS3OutpostsFullAccess

Descrição: Fornece acesso total ao Amazon S3 no Outposts por meio do. Console de gerenciamento da AWS

`AmazonS3OutpostsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonS3OutpostsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 02 de outubro de 2020, 17:26 UTC
- Hora da edição: 02 de outubro de 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3-outposts:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:ListTasks",
```

```
        "datasync:ListLocations",
        "datasync:DescribeTask",
        "datasync:DescribeLocation*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts",
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonS3OutpostsReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon S3 no Outposts por meio do. Console de gerenciamento da AWS

`AmazonS3OutpostsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonS3OutpostsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 02 de outubro de 2020, 18:55 UTC
- Hora da edição: 02 de outubro de 2020, 18:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3-outposts:Get*",
        "s3-outposts:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:ListTasks",
        "datasync:ListLocations",
        "datasync:DescribeTask",
        "datasync:DescribeLocation*"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts",
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonS3ReadOnlyAccess

Descrição: Fornece acesso somente para leitura a todos os buckets por meio do Console de gerenciamento da AWS.

`AmazonS3ReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonS3ReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 10 de agosto de 2023, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonS3TablesFullAccess

Descrição: fornece acesso total a todos os buckets da tabela do S3.

`AmazonS3TablesFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonS3TablesFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de dezembro de 2024, 15:21 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3TablesFullAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "PassRoleToS3TablesReplication",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "replication.s3tables.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonS3TablesLakeFormationServiceRole

Descrição: Essa política gerenciada concede ao AWS Lake Formation permissões para atuar em todos os compartimentos de tabelas, namespaces e tabelas da conta.

`AmazonS3TablesLakeFormationServiceRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonS3TablesLakeFormationServiceRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço

- Horário de criação: 19 de junho de 2025, 19:07 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3TablesLakeFormationServiceRole`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForS3ListTableBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3tables:ListTableBuckets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "s3tables:CreateTableBucket",
        "s3tables:GetTableBucket",
        "s3tables:CreateNamespace",
        "s3tables:GetNamespace",
```

```
        "s3tables:ListNamespaces",
        "s3tables:DeleteNamespace",
        "s3tables:DeleteTableBucket",
        "s3tables:CreateTable",
        "s3tables:DeleteTable",
        "s3tables:GetTable",
        "s3tables:ListTables",
        "s3tables:RenameTable",
        "s3tables:UpdateTableMetadataLocation",
        "s3tables:GetTableMetadataLocation",
        "s3tables:GetTableData",
        "s3tables:PutTableData",
        "s3tables:PutTableBucketEncryption"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSDataAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3tables:*:*:bucket/*/table/*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "KMSDescribeKeyAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3tables.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonS3TablesReadOnlyAccess

Descrição: fornece acesso somente leitura a todos os buckets da tabela do S3.

`AmazonS3TablesReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonS3TablesReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Horário de criação: 03 de dezembro de 2024, 15:21 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3TablesReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:Get*",
        "s3tables:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

Descrição: Política de função de serviço usada pelo serviço AWS service (Serviço da AWS) Catalog para provisionar produtos do SageMaker portfólio de produtos da Amazon. Concede permissões a um conjunto de serviços relacionados CodePipeline, incluindo CodeBuild, CodeCommit, CloudFormation Glue, etc.

`AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de novembro de 2020, 18:48 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPermission",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:PATCH",
        "apigateway:DELETE"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPostPermission",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:POST"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPatchPermission",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:PATCH"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnMutatePermission",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
      "Condition" : {
        "ArnLikeIfExists" : {
          "cloudformation:RoleArn" : [
            "arn:aws:sts::*:assumed-role/AmazonSageMakerServiceCatalog*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnTemplatePermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "cloudformation:ValidateTemplate"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:UpdateProject"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CreateCommit",
        "codecommit:CreateRepository",
        "codecommit:DeleteRepository",
        "codecommit:GetRepository",
        "codecommit:TagResource"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeCommitListPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodePipelinePermission",
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:CreatePipeline",
        "codepipeline:DeletePipeline",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
```

```
        "codepipeline:StartPipelineExecution",
        "codepipeline:TagResource",
        "codepipeline:UpdatePipeline"
      ],
      "Resource" : [
        "arn:aws:codepipeline:*:*:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCIAMUserPermission",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:CreateUserPool",
        "cognito-idp:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCIAMPermission",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteGroup",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:DeleteUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
```

```
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:DeleteRepository",
        "ecr:TagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogEventBridgePermission",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogFirehosePermission",
      "Effect" : "Allow",
      "Action" : [
        "firehose:CreateDeliveryStream",
        "firehose:DeleteDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "firehose:StartDeliveryStreamEncryption",
        "firehose:StopDeliveryStreamEncryption",
        "firehose:UpdateDestination"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    },
```

```
    {
      "Sid" : "AmazonSageMakerServiceCatalogGluePermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker-*",
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:userDefinedFunction/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueClassiferPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateClassifier",
        "glue:DeleteClassifier",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeleteTrigger",
        "glue:DeleteWorkflow",
        "glue:StopCrawler"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueWorkflowPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateWorkflow"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:workflow/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueJobPermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:CreateJob"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:job/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueCrawlerPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCrawler",
        "glue:GetCrawler"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:crawler/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueTriggerPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTrigger",
        "glue:GetTrigger"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:trigger/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerServiceCatalog*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogLambdaPermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:CreateFunction",
```

```
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogLambdaTagPermission",
      "Effect" : "Allow",
      "Action" : "lambda:TagResource",
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/apigateway/AccessLogs/*",
        "arn:aws:logs:*:*:log-group::log-stream:*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogS3ReadPermission",
```

```
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogS3ReadSagemakerResourcePermission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogS3MutatePermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:GetBucketPolicy",
        "s3:PutBucketAcl",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketCORS",
        "s3:PutBucketTagging",
        "s3:PutObjectTagging"
      ],
      "Resource" : "arn:aws:s3:::sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
```

```
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeWorkteam",
        "sagemaker:CreateCodeRepository",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:DeleteCodeRepository"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerImagePermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:CreateImage",
        "sagemaker:DeleteImage",
        "sagemaker:DescribeImage",
        "sagemaker:UpdateImage",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:image/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogStepFunctionPermission",
      "Effect" : "Allow",
      "Action" : [
        "states:CreateStateMachine",
        "states:DeleteStateMachine",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeStarPermission",
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : "codeconnections:PassConnection",
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerCanvasAIServicesAccess

Descrição: Fornece permissões para o Amazon SageMaker Canvas usar serviços de IA para oferecer suporte a soluções de IA prontas para uso. Essa política adicionará mais permissões mutantes para serviços à medida que o Amazon SageMaker Canvas adicionar suporte.

`AmazonSageMakerCanvasAIServicesAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerCanvasAIServicesAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de março de 2023, 22:36 UTC
- Hora da edição: 29 de novembro de 2023, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Textract",
      "Effect" : "Allow",
      "Action" : [
        "textract:AnalyzeDocument",
        "textract:AnalyzeExpense",
        "textract:AnalyzeID",
        "textract:StartDocumentAnalysis",
        "textract:StartExpenseAnalysis",
        "textract:GetDocumentAnalysis",
        "textract:GetExpenseAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Rekognition",
      "Effect" : "Allow",
      "Action" : [
        "rekognition:DetectLabels",
        "rekognition:DetectText"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Comprehend",
      "Effect" : "Allow",
      "Action" : [
        "comprehend:BatchDetectDominantLanguage",
        "comprehend:BatchDetectEntities",
        "comprehend:BatchDetectSentiment",
```

```
        "comprehend:DetectPiiEntities",
        "comprehend:DetectEntities",
        "comprehend:DetectSentiment",
        "comprehend:DetectDominantLanguage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Bedrock",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:ListFoundationModels",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateBedrockResourcesPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelCustomizationJob",
        "bedrock:CreateProvisionedModelThroughput",
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:model-customization-job/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker",
            "Canvas"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:RequestTag/Canvas" : "true",
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceTag/Canvas" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "GetStopAndDeleteBedrockResourcesPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetCustomModel",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:StopModelCustomizationJob",
        "bedrock:DeleteProvisionedModelThroughput"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:model-customization-job/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceTag/Canvas" : "true"
        }
      }
    },
    {
      "Sid" : "FoundationModelPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelCustomizationJob"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "BedrockFineTuningPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerCanvasBedrockAccess

Descrição: Essa política concede permissões para usar o Amazon Bedrock in SageMaker Canvas ao fornecer acesso a serviços downstream, como o S3.

`AmazonSageMakerCanvasBedrockAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerCanvasBedrockAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 2 de fevereiro de 2024, 18:37 UTC
- Hora da edição: 2 de fevereiro de 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3CanvasAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/Canvas",
        "arn:aws:s3:::sagemaker-*/Canvas/*"
      ]
    },
    {
      "Sid" : "S3BucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerCanvasDataPrepFullAccess

Descrição: Fornece acesso total aos SageMaker recursos e operações da Amazon para preparação de dados no Canvas. A política também fornece acesso selecionado a serviços relacionados (por exemplo, S3, IAM, KMS, RDS, CloudWatch Logs, Redshift, Athena, Glue, Secrets Manager). EventBridge Essa política deve ser anexada à função de execução do Amazon SageMaker Domain/ User Profile.

`AmazonSageMakerCanvasDataPrepFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerCanvasDataPrepFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de outubro de 2023, 22:56 UTC
- Hora da edição: 16 de agosto de 2024, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerListFeatureGroupOperation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListFeatureGroups",
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerFeatureGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateFeatureGroup",
        "sagemaker:DescribeFeatureGroup"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:feature-group/*"
    },
    {
      "Sid" : "SageMakerProcessingJobOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateProcessingJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:processing-job/*canvas-data-prep*"
    },
    {
      "Sid" : "SageMakerProcessingJobListOperation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListProcessingJobs",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPipelineOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribePipeline",
        "sagemaker:CreatePipeline",
        "sagemaker:UpdatePipeline",
        "sagemaker:DeletePipeline",
        "sagemaker:StartPipelineExecution",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:DescribePipelineExecution"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:pipeline/*canvas-data-prep*"
    },
    {
      "Sid" : "KMSListOperations",
      "Effect" : "Allow",
```

```
      "Action" : "kms:ListAliases",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetObjectOperation",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMListOperations",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetOperations",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassOperation",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EventBridgePutOperation",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeTagBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTagOperation",
      "Effect" : "Allow",
      "Action" : "events:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
```

```
        "glue:GetTable",
        "glue:GetTables",
        "glue:SearchTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "EMROperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups"
      ],
      "Resource" : "arn:aws:elasticmapreduce:*:*:cluster/*"
    },
    {
      "Sid" : "EMRListOperation",
      "Effect" : "Allow",
      "Action" : "elasticmapreduce:ListClusters",
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaListDataCatalogOperation",
      "Effect" : "Allow",
      "Action" : "athena:ListDataCatalogs",
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaQueryExecutionOperations",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*"
    },
    {
      "Sid" : "AthenaDataCatalogOperations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*"
    },
    {
      "Sid" : "RedshiftOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftArnBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "arn:aws:redshift:*:*:cluster:*"
    },
    {
      "Sid" : "RedshiftGetCredentialsOperation",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "SecretsManagerARNBasedOperation",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
    },
    {
      "Sid" : "SecretManagerTagBasedOperation",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "LoggingOperation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/studio:*"
    },
    {
      "Sid" : "EMRServerlessCreateApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:CreateApplication",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListApplicationOperation",
      "Effect" : "Allow",
```

```
      "Action" : "emr-serverless:ListApplications",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessApplicationOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:UpdateApplication",
        "emr-serverless:GetApplication"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessStartJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:StartJobRun",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListJobRuns",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "EMRServerlessJobRunOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetJobRun",
        "emr-serverless:CancelJobRun"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*/jobruns/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessTagResourceOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:TagResource",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassOperationForEMRServerless",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerCanvasEMRSExecutionAccess-*",
        "arn:aws:iam::*:role/AmazonSageMakerCanvasEMRSExecutionAccess-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerCanvasDirectDeployAccess

Descrição: permite que o Amazon SageMaker Canvas crie, gerencie e visualize detalhes de endpoints para endpoints criados por meio do Canvas. Permite que o Amazon SageMaker Canvas recupere métricas de invocação de endpoints do. CloudWatch

`AmazonSageMakerCanvasDirectDeployAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerCanvasDirectDeployAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 06 de outubro de 2023, 18:11 UTC
- Hora da edição: 06 de outubro de 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerEndpointPerms",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:InvokeEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:Canvas*",
        "arn:aws:sagemaker:*:*:canvas*"
      ]
    },
    {
      "Sid" : "ReadCWInvocationMetrics",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy

Descrição: Essa política concede permissões ao Amazon EMR Serverless para serviços como o S3, usado pelo Amazon SageMaker Canvas para processamento de grandes dados.

`AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de julho de 2024, 0:35 UTC
- Hora da edição: 27 de julho de 2024, 0:35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
```

```
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetObjectOperation",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerCanvasForecastAccess

Descrição: Essa política concede as permissões normalmente necessárias para usar o SageMaker Canvas com o Amazon Forecast.

`AmazonSageMakerCanvasForecastAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerCanvasForecastAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 24 de agosto de 2022, 20:04 UTC
- Hora da edição: 24 de agosto de 2022, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/Canvas*",
        "arn:aws:s3:::sagemaker-*/canvas*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerCanvasFullAccess

Descrição: Fornece acesso total aos recursos e operações do Amazon SageMaker Canvas. A política também fornece acesso selecionado a serviços relacionados (por exemplo, S3, IAM, VPC,

ECR, CloudWatch Logs, Redshift, Secrets Manager e Forecast). Essa política deve ser anexada à função de execução do Amazon SageMaker Domain/User Profile.

`AmazonSageMakerCanvasFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerCanvasFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de setembro de 2022, 0:44 UTC
- Hora da edição: 16 de agosto de 2024, 4:35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess`

Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerUserDetailsAndPackageOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListTags",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListEndpoints"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPackageGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelPackage"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*"
      ]
    },
    {
      "Sid" : "SageMakerTrainingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:AddTags",
```

```
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*Canvas*",
        "arn:aws:sagemaker:*:*:*canvas*",
        "arn:aws:sagemaker:*:*:*model-compilation-*"
      ]
    },
    {
      "Sid" : "SageMakerHostingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteModel",
        "sagemaker:InvokeEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:InvokeEndpointAsync"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*Canvas*",
        "arn:aws:sagemaker:*:*:*canvas*"
      ]
    },
    {
      "Sid" : "EC2VPCOperation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECROperations",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetAuthorizationToken"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetOperations",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassOperation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LoggingOperation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:CreateBucket",
        "s3:GetBucketCors",
        "s3:GetBucketLocation"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "ReadSageMakerJumpstartArtifacts",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
      ]
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : "glue:SearchTables",
      "Resource" : [
        "arn:aws:glue:*:*:table/*/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "SecretsManagerARNBasedOperation",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "SecretManagerTagBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftGetCredentialsOperation",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
```

```
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "ForecastOperations",
      "Effect" : "Allow",
      "Action" : [
        "forecast:CreateExplainabilityExport",
        "forecast:CreateExplainability",
        "forecast:CreateForecastEndpoint",
        "forecast:CreateAutoPredictor",
        "forecast:CreateDatasetImportJob",
        "forecast:CreateDatasetGroup",
        "forecast:CreateDataset",
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast:CreatePredictorBacktestExportJob",
        "forecast:CreatePredictor",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeExplainability",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeForecastEndpoint",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeDataset",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:GetAccuracyMetrics",
        "forecast:InvokeForecastEndpoint",
        "forecast:GetRecentForecastContext",
        "forecast:DescribePredictor",
        "forecast:TagResource",
        "forecast:DeleteResourceTree"
      ],
      "Resource" : [
        "arn:aws:forecast:*:*:*Canvas*"
      ]
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
```

```
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassOperationForForecast",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AutoscalingOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "sagemaker",
          "application-autoscaling:scalable-dimension" :
"sagemaker:variant:DesiredInstanceCount"
        }
      }
    },
    {
      "Sid" : "AsyncEndpointOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "sagemaker:DescribeEndpointConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeScalingOperations",
      "Effect" : "Allow",
```

```
      "Action" : [
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerCloudWatchUpdate",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AutoscalingSageMakerEndpointOperation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AthenaOperation",
      "Action" : [
        "athena:ListTableMetadata",
        "athena:ListDataCatalogs",
        "athena:ListDatabases"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueOperation",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTables"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QuicksightOperation",
      "Action" : [
        "quicksight:ListNamespaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowUseOfKeyInAccount",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Source" : "SageMakerCanvas",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessCreateApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:CreateApplication",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListApplications",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessApplicationOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:UpdateApplication",
        "emr-serverless:StopApplication",
        "emr-serverless:GetApplication",
        "emr-serverless:StartApplication"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessStartJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:StartJobRun",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListJobRuns",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessJobRunOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetJobRun",
        "emr-serverless:CancelJobRun"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*/jobruns/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "EMRServerlessTagResourceOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:TagResource",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassOperationForEMRServerless",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerCanvasEMRSExecutionAccess-*",
        "arn:aws:iam::*:role/AmazonSageMakerCanvasEMRSExecutionAccess-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerCanvasSMDataScienceAssistantAccess

Descrição: Fornece permissões para o Amazon SageMaker Canvas usar o serviço SageMaker Data Science Assistant. Atualmente, o Data Science Assistant usa a Amazon SageMaker e o Amazon Q Developer para processar solicitações de usuários.

`AmazonSageMakerCanvasSMDataScienceAssistantAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerCanvasSMDataScienceAssistantAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 04 de dezembro de 2024, 14:06 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasSMDataScienceAssistantAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerDataScienceAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker-data-science-assistant:SendConversation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmazonQDeveloperAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerCapacityReservationServiceRolePolicy

Descrição: Essa política concede permissões às reservas de SageMaker capacidade da Amazon para publicar CloudWatch métricas nas contas dos clientes para visibilidade da utilização.

`AmazonSageMakerCapacityReservationServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 08 de abril de 2026, 20:27 UTC
- Horário editado: 08 de abril de 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCapacityReservationServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudwatchPutMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "aws/sagemaker/CapacityReservations"
        }
```

```
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerClusterInstanceRolePolicy

Descrição: Essa política concede as permissões normalmente necessárias para usar o Amazon SageMaker Cluster.

`AmazonSageMakerClusterInstanceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerClusterInstanceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2023, 15:11 UTC
- Hora da edição: 29 de novembro de 2023, 15:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudwatchLogStreamPublishPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*:log-stream:*"
      ]
    },
    {
      "Sid" : "CloudwatchLogGroupCreationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*"
      ]
    },
    {
      "Sid" : "CloudwatchPutMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "/aws/sagemaker/Clusters"
        }
      }
    },
    {
```

```
      "Sid" : "DataRetrievalFromS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SSMConnectivityPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerCoreServiceRolePolicy

Descrição: Política gerenciada para Service Linked Role for Amazon SageMaker Core Services

`AmazonSageMakerCoreServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 21 de dezembro de 2020, 21:40 UTC
- Hora da edição: 21 de dezembro de 2020, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:AuthorizedService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerEdgeDeviceFleetPolicy

Descrição: Fornece as permissões necessárias para que o SageMaker Edge crie e gerencie uma frota de dispositivos para o cliente usando a conexão de nuvem padrão.

`AmazonSageMakerEdgeDeviceFleetPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerEdgeDeviceFleetPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 08 de dezembro de 2020, 16:17 UTC
- Hora da edição: 08 de dezembro de 2020, 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeviceS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "SageMakerEdgeApis",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:SendHeartbeat",
        "sagemaker:GetDeviceRegistration"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateIoTRoleAlias",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateRoleAlias",
        "iot:DescribeRoleAlias",
        "iot:UpdateRoleAlias",
        "iot:ListTagsForResource",
        "iot:TagResource"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:rolealias/SageMakerEdge*"
      ]
    },
    {
      "Sid" : "CreateIoTRoleAliasIamPermissionsGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*",
        "arn:aws:iam::*:role/*Sagemaker*",
        "arn:aws:iam::*:role/*sagemaker*"
      ]
    },
    {
      "Sid" : "CreateIoTRoleAliasIamPermissionsPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*",
        "arn:aws:iam::*:role/*Sagemaker*",
        "arn:aws:iam::*:role/*sagemaker*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com",
```

```
            "credentials.iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerFeatureStoreAccess

Descrição: Fornece as permissões necessárias para habilitar a loja offline para um grupo de SageMaker FeatureStore recursos da Amazon.

`AmazonSageMakerFeatureStoreAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerFeatureStoreAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2020, 16:24 UTC
- Hora da edição: 05 de dezembro de 2022, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*/metadata/*",
        "arn:aws:s3:::*Sagemaker*/metadata/*",
        "arn:aws:s3:::*sagemaker*/metadata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*"
```

```
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerFullAccess

Descrição: Fornece acesso total à Amazon SageMaker por meio do Console de gerenciamento da AWS SDK e. Também fornece acesso selecionado a serviços relacionados (por exemplo, S3, ECR, CloudWatch Logs).

`AmazonSageMakerFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2017, 13:07 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFullAccess`

Versão da política

Versão da política: v29 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:partner-app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*",
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AllowAddTagsForSpace",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:space/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateSpace"
        }
      }
    },
    {
```

```
      "Sid" : "AllowAddTagsForApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*"
      ]
    },
    {
      "Sid" : "AllowUseOfTrainingPlanResources",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateCluster",
        "sagemaker:UpdateCluster",
        "sagemaker:DescribeTrainingPlan"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AllowStudioActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListUserProfiles",
        "sagemaker:DescribeSpace",
        "sagemaker:ListSpaces",
        "sagemaker:DescribeApp",
        "sagemaker:ListApps"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppActionsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
```

```
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAppActionsForSharedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private",
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
```

```
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "cognito-idp:AdminAddUserToGroup",
        "cognito-idp:AdminCreateUser",
        "cognito-idp:AdminDeleteUser",
        "cognito-idp:AdminDisableUser",
        "cognito-idp:AdminEnableUser",
        "cognito-idp:AdminRemoveUserFromGroup",
        "cognito-idp:CreateGroup",
```

```
        "cognito-idp:CreateUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:List*",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:CreateRepository",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:StartImageScan",
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "glue:CreateJob",
        "glue:DeleteJob",
        "glue:GetJob*",
        "glue:GetTable*",
        "glue:GetWorkflowRun",
        "glue:ResetJobBookmark",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:UpdateJob",
        "groundtruthlabeling:*",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
```

```
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery",
        "robomaker:CreateSimulationApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:DeleteSimulationApplication",
        "robomaker:CreateSimulationJob",
        "robomaker:DescribeSimulationJob",
        "robomaker:CancelSimulationJob",
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/*sagemaker*"
```

```
      ]
    },
    {
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:*sagemaker*",
        "arn:aws:codecommit:*:*:*SageMaker*",
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowStepFunctionsActions",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowSecretManagerActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "AllowReadOnlySecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
```

```
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*",
        "arn:aws:s3:::*aws-glue*"
      ]
    },
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3BucketACL",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
```

```
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForRobomaker",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonSageMaker*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "robomaker.amazonaws.com",
            "states.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueCreateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable"
      ],
```

```
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueUpdateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore"
      ]
    },
    {
      "Sid" : "AllowGlueDeleteTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetTablesAndDatabases",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
```

```
    },
    {
      "Sid" : "AllowGlueGetAndCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:database/sagemaker_processing",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/sagemaker_data_wrangler"
      ]
    },
    {
      "Sid" : "AllowRedshiftDataActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowListTagsForUserProfile",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*"
      ]
    },
    {
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AllowS3ExpressObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateSession"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*",
        "arn:aws:s3express:*:*:bucket/*aws-glue*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressCreateBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressListBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:ListAllMyDirectoryBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerGeospatialExecutionRole

Descrição: Essa política fornece acesso a serviços que normalmente são necessários para o uso SageMaker geoespacial.

`AmazonSageMakerGeospatialExecutionRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerGeospatialExecutionRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço

- Hora da criação: 30 de novembro de 2022, 10:08 UTC
- Hora da edição: 10 de maio de 2023, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:GetEarthObservationJob",
      "Resource" : "arn:aws:sagemaker-geospatial:*:*:earth-observation-job/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:GetRasterDataCollection",
```

```
      "Resource" : "arn:aws:sagemaker-geospatial:*:*:raster-data-collection/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerGeospatialFullAccess

Descrição: Essa política concede permissões que permitem acesso total à Amazon SageMaker Geospatial por meio do SDK Console de gerenciamento da AWS e.

`AmazonSageMakerGeospatialFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerGeospatialFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 30 de novembro de 2022, 10:06 UTC
- Hora da edição: 30 de novembro de 2022, 10:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker-geospatial.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerGroundTruthExecution

Descrição: Fornece acesso aos AWS serviços necessários para executar o trabalho de SageMaker GroundTruth etiquetagem

`AmazonSageMakerGroundTruthExecution` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerGroundTruthExecution` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de julho de 2020, 19:30 UTC
- Hora da edição: 29 de abril de 2022, 20:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CustomLabelingJobs",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*GtRecipe*",
```

```
        "arn:aws:lambda:*:*:function:*LabelingFunction*",
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*GroundTruth*",
        "arn:aws:s3:::*Groundtruth*",
        "arn:aws:s3:::*groundtruth*",
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StreamingQueue",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:*GroundTruth*"
    },
    {
      "Sid" : "StreamingTopicSubscribe",
      "Effect" : "Allow",
      "Action" : "sns:Subscribe",
      "Resource" : [
        "arn:aws:sns:*:*:*GroundTruth*",
        "arn:aws:sns:*:*:*Groundtruth*",
        "arn:aws:sns:*:*:*groundTruth*",
        "arn:aws:sns:*:*:*groundtruth*",
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sageMaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sns:Protocol" : "sqs"
        },
        "StringLike" : {
          "sns:Endpoint" : "arn:aws:sqs:*:*:*GroundTruth*"
```

```
        }
      }
    },
    {
      "Sid" : "StreamingTopic",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*GroundTruth*",
        "arn:aws:sns:*:*:*Groundtruth*",
        "arn:aws:sns:*:*:*groundTruth*",
        "arn:aws:sns:*:*:*groundtruth*",
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sageMaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "StreamingTopicUnsubscribe",
      "Effect" : "Allow",
      "Action" : [
        "sns:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "WorkforceVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ec2:VpceServiceName" : [
            "*sagemaker-task-resources*",
            "aws.sagemaker*labeling*"
          ]
        }
```

```
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerHyperPodGatedModelAccess

Descrição: Essa política gerenciada da Amazon fornece as permissões necessárias SageMaker HyperPod para acessar modelos fechados no SageMaker Jumpstart. Ele permite criar URLs pré-assinados para o conteúdo do hub no Hub SageMaker público.

`AmazonSageMakerHyperPodGatedModelAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerHyperPodGatedModelAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 17 de janeiro de 2026, 01:04 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodGatedModelAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreatePresignedUrlAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateHubContentPresignedUrls"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:hub/SageMakerPublicHub",
        "arn:aws:sagemaker:*:*:hub-content/SageMakerPublicHub/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerHyperPodInferenceAccess

Descrição: Essa política fornece os privilégios administrativos necessários para configurar o operador de SageMaker HyperPod inferência. Ele permite que o operador de inferência acesse recursos AWS

de rede, Amazon S3, Amazon ECR, Amazon CloudWatch, AWS Certificate Manager e SageMaker recursos necessários para implantar e gerenciar cargas de trabalho de inferência em clusters HyperPod

`AmazonSageMakerHyperPodInferenceAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerHyperPodInferenceAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 27 de janeiro de 2026, 20:34 UTC
- Horário editado: 20 de julho de 2026, 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodInferenceAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeleteObjectsPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::hyperpod-tls*/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::hyperpod-tls*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "s3:ExistingObjectTag/CreatedBy" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "S3PutObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectTagging"
      ],
      "Resource" : [
        "arn:aws:s3:::hyperpod-tls*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "s3:RequestObjectTag/CreatedBy" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "DataCaptureS3",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : [
```

```
        "arn:aws:s3:::hyperpod-tls*/data-capture/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3ListBucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::hyperpod-tls*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataCaptureKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com",
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::hyperpod-tls*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ECRAuthorization",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECRRepositoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*"
    },
    {
      "Sid" : "EC2DescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2NetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EKSClusterAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EKSAccessEntryPolicyAssociation",
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
        "StringEquals" : {
          "eks:policyarn" : "arn:aws:eks::aws:cluster-access-policy/
AmazonSagemakerHyperpodInferenceMonitoringPolicy"
        }
      }
    },
    {
      "Sid" : "EKSAccessEntryListPolicies",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ELBListAndDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FSxAccess",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CertificateImportPermission",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:ImportCertificate"
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CreatedBy"
        },
        "StringEquals" : {
```

```
          "aws:RequestTag/CreatedBy" : "HyperPodInference",
          "aws:ResourceTag/CreatedBy" : "HyperPodInference",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CertificateDeletePermission",
      "Effect" : "Allow",
      "Action" : "acm:DeleteCertificate",
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerHyperPodInference*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchMetricsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "HyperPodInference"
        }
      }
    },
```

```
    {
      "Sid" : "CloudWatchLogsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeModel",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeClusterInference",
        "sagemaker:UpdateClusterInference",
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpointconfig/*",
        "arn:aws:sagemaker:*:*:cluster/*",
        "arn:aws:sagemaker:*:*:hub-content/*",
        "arn:aws:sagemaker:*:*:hub/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "SageMakerCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModel",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "SageMakerTagging",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : [
            "CreateModel",
            "CreateEndpointConfig",
            "CreateEndpoint"
          ]
        }
      }
    },
    {
      "Sid" : "SageMakerDeleteAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteModel",
```

```
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "HyperPodInference"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerHyperPodInferenceGatewayAccess

Descrição: Essa política fornece as permissões necessárias para configurar e operar o gateway de SageMaker HyperPod inferência. Ele permite que o gateway gerencie certificados do AWS Certificate Manager (ACM) para encerramento de TLS ao implantar e servir cargas de trabalho de inferência em clusters. HyperPod

`AmazonSageMakerHyperPodInferenceGatewayAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerHyperPodInferenceGatewayAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 09 de setembro de 2026, 23:27 UTC
- Horário editado: 09 de setembro de 2026, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodInferenceGatewayAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ImportOwnedCert",
      "Effect" : "Allow",
      "Action" : [
        "acm:ImportCertificate",
        "acm:AddTagsToCertificate"
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "HyperPodInference",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "CreatedBy"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "ReadOwnedCerts",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:ListTagsForCertificate"
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "HyperPodInference",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeleteOwnedImportedCerts",
      "Effect" : "Allow",
      "Action" : [
        "acm:DeleteCertificate"
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "HyperPodInference",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "acm:CertificateKeyPairOrigin" : "CUSTOMER_PROVIDED"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerHyperPodObservabilityAdminAccess

Descrição: Essa política fornece privilégios administrativos necessários para configurar a SageMaker HyperPod observabilidade. Ela permite o acesso ao Amazon Managed Prometheus, ao Amazon Managed Grafana e ao EKS Addons. A política também inclui amplo acesso às APIs HTTP do Grafana ServiceAccountTokens em todos os espaços de trabalho do Amazon Managed Grafana em sua conta.

`AmazonSageMakerHyperPodObservabilityAdminAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerHyperPodObservabilityAdminAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 10 de julho de 2025, 14:37 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodObservabilityAdminAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrometheusCreateAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "aps:CreateWorkspace"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "PrometheusTagsAccess",
      "Effect" : "Allow",
      "Action" : "aps:TagResource",
      "Resource" : [
        "arn:aws:aps:*:*:/workspaces",
        "arn:aws:aps:*:*:rulegroupsnamespace/*/HyperPodObservabilityNamespace"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "PrometheusDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:DescribeWorkspace"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*"
    },
    {
      "Sid" : "PrometheusListAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:ListWorkspaces"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "PrometheusAlertsRuleGroupAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateAlertManagerDefinition",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeRuleGroupsNamespace",
        "aps:ListRuleGroupsNamespaces"
      ],
      "Resource" : [
        "arn:aws:aps:*:*:workspace/*",
        "arn:aws:aps:*:*:rulegroupsnamespace/*/HyperPodObservabilityNamespace"
      ]
    },
    {
      "Sid" : "PrometheusCreateRuleGroupAccess",
      "Effect" : "Allow",
      "Action" : "aps:CreateRuleGroupsNamespace",
      "Resource" : "arn:aws:aps:*:*:rulegroupsnamespace/*/
HyperPodObservabilityNamespace",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "GrafanaCreateWorkspaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:CreateWorkspace"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "GrafanaTagsAccess",
```

```
      "Effect" : "Allow",
      "Action" : "grafana:TagResource",
      "Resource" : "arn:aws:grafana:*:*:/workspaces",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "GrafanaListAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:ListWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaServiceAccountAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:CreateWorkspaceApiKey",
        "grafana:CreateWorkspaceServiceAccount",
        "grafana:CreateWorkspaceServiceAccountToken",
        "grafana:ListWorkspaceServiceAccounts",
        "grafana:ListWorkspaceServiceAccountTokens",
        "grafana:DeleteWorkspaceServiceAccountToken"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces/*"
    },
    {
      "Sid" : "IAMGrafanaPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityGrafanaAccess-*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "grafana.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMEKSPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityAddonAccess-*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMGetRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityAddonAccess-*"
      ]
    },
    {
      "Sid" : "HyperPodClusterAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListClusters",
        "sagemaker:DescribeCluster"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "EKSAddonAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeleteAddon",
        "eks:UpdateAddon",
        "eks:DescribeAddon"
      ],
      "Resource" : "arn:aws:eks:*:*:addon/*/amazon-sagemaker-hyperpod-observability/*"
    },
    {
      "Sid" : "EKSAddonDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeAddonConfiguration",
        "eks:DescribeAddonVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSAddonPodIdentityAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribePodIdentityAssociation",
        "eks:DeletePodIdentityAssociation",
        "eks:UpdatePodIdentityAssociation"
      ],
      "Resource" : "arn:aws:eks:*:*:podidentityassociation/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "EKSListDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListAddons",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
```

```
      "Sid" : "EKSCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateAddon",
        "eks:CreatePodIdentityAssociation"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "EKSTagsAccess",
      "Effect" : "Allow",
      "Action" : "eks:TagResource",
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:eks:*:*:addon/*/*/*",
        "arn:aws:eks:*:*:podidentityassociation/*/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "SSOAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:CreateManagedApplicationInstance"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerHyperPodServiceRolePolicy

Descrição: Essa política concede permissões à Amazon SageMaker HyperPod para AWS serviços relacionados, como Amazon EKS, Amazon CloudWatch etc.

`AmazonSageMakerHyperPodServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 6 de setembro de 2024, 17:04 UTC
- Hora da edição: 6 de setembro de 2024, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerHyperPodServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EKSClusterDescribePermissions",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogStreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*:log-stream:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
```

```
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerHyperPodTrainingOperatorAccess

Descrição: Essa política fornece as permissões administrativas necessárias para configurar o operador SageMaker HyperPod de treinamento. Ele permite o acesso aos complementos Amazon SageMaker HyperPod e EKS. A política inclui permissões para descrever os SageMaker HyperPod recursos em sua conta.

`AmazonSageMakerHyperPodTrainingOperatorAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerHyperPodTrainingOperatorAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 19 de agosto de 2025, 17:04 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodTrainingOperatorAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribeClusterNodeOnHyperPodClusters",
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeClusterNode",
      "Resource" : "arn:aws:sagemaker:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerInferenceServiceRolePolicy

Descrição: Política gerenciada para Service Linked Role for Amazon SageMaker Inference.

`AmazonSageMakerInferenceServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 30 de julho de 2026, 19:42 UTC
- Horário editado: 17 de agosto de 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerInferenceServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateENIWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonSageMakerManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "CreateENIInSubnetAndSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "CreateENIPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Permission" : "INSTANCE-ATTACH",
          "aws:ResourceTag/AmazonSageMakerManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "DeleteENITagScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonSageMakerManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "DeleteENIPermissionTagScoped",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonSageMakerManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "TagOnCreateSageMakerResourcesForENI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface",
          "aws:RequestTag/AmazonSageMakerManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DescribeNetworkResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
```

```
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerJobFullAccess

Descrição: fornece permissões para que as funções de execução de SageMaker tarefas da Amazon acessem dados no Amazon S3, invoquem agentes por meio do Amazon Bedrock AgentCore, acompanhem experimentos com o MLflow, publiquem pacotes de modelos, gravem logs na Amazon CloudWatch, invoquem funções do AWS Lambda e gerenciem interfaces de rede Amazon VPC.

`AmazonSageMakerJobFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerJobFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de junho de 2026, 02:42 UTC
- Horário editado: 03 de junho de 2026, 02:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerJobFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:hub/*",
        "arn:aws:sagemaker:*:*:hub-content/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerModelPackagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AccessModelPackage",
        "sagemaker:CreateModelPackage",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MLflowPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:DescribeMlflowApp",
        "sagemaker:CallMlflowAppApi",
        "sagemaker-mlflow:CreateExperiment",
        "sagemaker-mlflow:CreateRun",
        "sagemaker-mlflow:UpdateRun",
        "sagemaker-mlflow:LogBatch",
        "sagemaker-mlflow:GetExperimentByName",
        "sagemaker-mlflow:GetMetricHistory",
        "sagemaker-mlflow:GetRun",
        "sagemaker-mlflow:StartTrace",
        "sagemaker-mlflow:EndTrace",
        "sagemaker-mlflow:SearchTraces",
        "sagemaker-mlflow:ListArtifacts"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:mlflow-app/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:InvokeAgentRuntime",
        "bedrock-agentcore:StopRuntimeSession",
        "bedrock-agentcore:GetAgentRuntime"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:runtime/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2NetworkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeDhcpOptions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2NetworkInterfaceTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "EC2NetworkInterfaceDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerJobRuntimeAccess

Descrição: fornece permissões para que os tempos de execução do agente invoquem as APIs de tempo de execução de SageMaker tarefas da Amazon usadas durante a personalização do modelo para geração de amostras, conclusão da trajetória e envio de recompensas.

`AmazonSageMakerJobRuntimeAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerJobRuntimeAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de junho de 2026, 02:42 UTC
- Horário editado: 07 de agosto de 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerJobRuntimeAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerJobRuntimePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Sample",
        "sagemaker:SampleWithResponseStream",
        "sagemaker:CompleteRollout",
        "sagemaker:UpdateReward"
```

```
      ],
      "Resource" : "arn:aws:sagemaker:*:*:job/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BearerTokenPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CallWithBearerToken"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSPermissionsForMTRLRuntime",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerMechanicalTurkAccess

Descrição: Fornece acesso para criar FlowDefinition recursos de IA aumentada da Amazon contra qualquer equipe de trabalho.

`AmazonSageMakerMechanicalTurkAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerMechanicalTurkAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 03 de dezembro de 2019, 16:19 UTC
- Hora da edição: 03 de dezembro de 2019, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerModelCustomizationCoreAccess

Descrição: Concede permissões para fluxos de trabalho de personalização de SageMaker modelos, incluindo treinamento sem servidor, função de recompensa personalizada para aprendizado por reforço, avaliação de modelos e implantação em endpoints ou Bedrock. SageMaker

`AmazonSageMakerModelCustomizationCoreAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerModelCustomizationCoreAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 26 de maio de 2026, 18:57 UTC
- Horário editado: 21 de julho de 2026, 19:57 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelCustomizationCoreAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerPublicHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListHubContents"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
    {
      "Sid" : "SageMakerHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ImportHubContent",
        "sagemaker:ListHubs",
        "sagemaker:ListHubContents",
        "sagemaker:ListHubContentVersions",
        "sagemaker:DescribeHubContent",
        "sagemaker:DeleteHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:hub/*",
        "arn:aws:sagemaker:*:*:hub-content/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "JumpStartS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::jumpstart*"
      ]
    },
    {
      "Sid" : "SageMakerTrainingJob",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:ListTrainingJobs",
        "sagemaker:StopTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerMLFlow",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateMlflowApp",
        "sagemaker:DescribeMlflowApp",
        "sagemaker:CreatePresignedMlflowAppUrl",
        "sagemaker:CallMlflowAppApi",
        "sagemaker-mlflow:AccessUI",
        "sagemaker-mlflow:GetExperiment",
        "sagemaker-mlflow:GetExperimentByName",
```

```
        "sagemaker-mlflow:GetRun",
        "sagemaker-mlflow:GetMetricHistory",
        "sagemaker-mlflow:GetLoggedModel",
        "sagemaker-mlflow:SearchExperiments",
        "sagemaker-mlflow:SearchRuns",
        "sagemaker-mlflow:ListArtifacts",
        "sagemaker-mlflow:CreateExperiment",
        "sagemaker-mlflow:CreateRun",
        "sagemaker-mlflow:LogBatch",
        "sagemaker-mlflow:LogMetric",
        "sagemaker-mlflow:LogParam",
        "sagemaker-mlflow:LogModel",
        "sagemaker-mlflow:LogInputs",
        "sagemaker-mlflow:SetTag",
        "sagemaker-mlflow:UpdateRun"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:mlflow-app/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BYODataSetS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "SageMakerModelPackage",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:UpdateModelPackage",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:DescribeModel",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package-group/*",
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerLineage",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateAction",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateContext",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:QueryLineage",
        "sagemaker:AddAssociation",
        "sagemaker:UpdateArtifact"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:action/*",
        "arn:aws:sagemaker:*:*:artifact/*",
```

```
        "arn:aws:sagemaker:*:*:context/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:experiment-trial-component/*",
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:pipeline/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerPipelines",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePipeline",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:UpdatePipeline",
        "sagemaker:StartPipelineExecution"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:pipeline/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerInference",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateInferenceComponent",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DeleteInferenceComponent",
        "sagemaker:DeleteEndpoint",
```

```
        "sagemaker:InvokeEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:inference-component/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerInferenceAutoscaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerInferenceEcrReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListActions",
```

```
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListEndpoints",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListMlflowApps",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListWorkforces",
        "sagemaker:Search"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerTagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package-group/*",
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:hub/*",
        "arn:aws:sagemaker:*:*:hub-content/*",
        "arn:aws:sagemaker:*:*:training-job/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:inference-component/*",
        "arn:aws:sagemaker:*:*:action/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "SageMakerJobAdvancedSettings",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "ec2:DescribeVpcs",
        "servicequotas:ListServiceQuotas"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/*",
        "arn:aws:logs:*:*:log-group::log-stream:"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
```

```
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaListFunctions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaPermissionsForRewardFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:InvokeFunction",
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "LambdaLayerForAWSSDK",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetLayerVersion"
      ],
      "Resource" : [
        "arn:aws:lambda:*:336392948345:layer:AWSSDK*"
      ]
    },
    {
      "Sid" : "BedrockCustomModelAndEvaluation",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateCustomModel",
        "bedrock:CreateEvaluationJob",
        "bedrock:GetCustomModel",
        "bedrock:GetModelImportJob",
        "bedrock:GetImportedModel",
        "bedrock:GetEvaluationJob",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:evaluation-job/*",
        "arn:aws:bedrock:*:*:imported-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:model-import-job/*",
        "arn:aws:bedrock:*:*:foundation-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockModelImportAndList",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelImportJob",
        "bedrock:ListProvisionedModelThroughputs",
        "bedrock:ListCustomModelDeployments",
        "bedrock:ListCustomModels",
        "bedrock:ListModelImportJobs"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockFoundationModelOperations",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModelAvailability",
        "bedrock:ListFoundationModels"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PassRoleForSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/*SageMaker*",
        "arn:aws:iam::*:role/service-role/*Sagemaker*",
        "arn:aws:iam::*:role/service-role/*sagemaker*"
      ],
      "Condition" : {
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:sagemaker:*:*:*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "job.sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "PassRoleForAWSLambda",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SageMakerForLambda*",
        "arn:aws:iam::*:role/service-role/SageMakerForLambda*"
      ],
      "Condition" : {
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:lambda:*:*:function:*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassRoleForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SageMakerForBedrock*",
        "arn:aws:iam::*:role/service-role/SageMakerForBedrock*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerModelGovernanceUseAccess

Descrição: Essa política AWS gerenciada concede as permissões necessárias para usar todos os recursos do Amazon SageMaker Governance. A política também fornece acesso seleto a serviços relacionados (por exemplo, S3, KMS).

`AmazonSageMakerModelGovernanceUseAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerModelGovernanceUseAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de novembro de 2022, 8:58 UTC
- Hora da edição: 4 de junho de 2024, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSMMonitoringModelCards",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:UpdateMonitoringAlert",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:ListMonitoringAlertHistory",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:CreateModelCard",
        "sagemaker:DescribeModelCard",
        "sagemaker:UpdateModelCard",
        "sagemaker:DeleteModelCard",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelCardVersions",
        "sagemaker:CreateModelCardExportJob",
        "sagemaker:DescribeModelCardExportJob",
        "sagemaker:ListModelCardExportJobs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSMTrainingModelsSearchTags",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTrainingJobs",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:ListModels",
        "sagemaker:DescribeModel",
        "sagemaker:Search",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags",
        "sagemaker:ListTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowS3Actions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:CreateBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowS3ListActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerModelRegistryFullAccess

Descrição: esta é uma nova política gerenciada para o Registro de Modelos no Sagemaker. Essa política é uma política independente que pode ser anexada à função do usuário para acessar as funcionalidades relacionadas ao Registro de Modelos no Sagemaker.

`AmazonSageMakerModelRegistryFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerModelRegistryFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 13 de abril de 2023, 5:20 UTC
- Hora da edição: 6 de junho de 2024, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerModelRegistrySageMakerReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeAction",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:ListAssociations",
        "sagemaker:ListArtifacts",
        "sagemaker:ListModelMetadata",
```

```
        "sagemaker:ListModelPackages",
        "sagemaker:Search",
        "sagemaker:GetSearchSuggestions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistrySageMakerWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteTags",
        "sagemaker:UpdateModelPackage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryS3GetPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryS3ListPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryECRReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:DescribeImages"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryIAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryTagReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupGetPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupListPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "sagemaker:collection"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupDeletePermission",
      "Effect" : "Allow",
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:collection" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceKMSPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerNotebooksServiceRolePolicy

Descrição: Política gerenciada para Service Linked Role para Amazon SageMaker Notebooks

`AmazonSageMakerNotebooksServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 18 de outubro de 2019, 20:27 UTC
- Horário editado: 16 de abril de 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFSxDescribe",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerDeleteApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*"
    },
    {
      "Sid" : "AllowEFSAccessPointCreation",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateAccessPoint",
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*",
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
```

```
      "Sid" : "AllowEFSAccessPointDeletion",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DeleteAccessPoint"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:access-point/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSCreation",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateFileSystem",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSMountWithDeletion",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
```

```
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEFSTagging",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:TagResource",
      "Resource" : [
        "arn:aws:elasticfilesystem:*:*:access-point/*",
        "arn:aws:elasticfilesystem:*:*:file-system/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEC2Tagging",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "AllowEC2Operations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowEC2AuthZ",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowIdcOperations",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateManagedApplicationInstance",
        "sso:DeleteManagedApplicationInstance",
        "sso:GetManagedApplicationInstance"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSagemakerProfileCreation",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSagemakerSpaceOperationsForCanvasManagedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DescribeSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:ListTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*"
    },
    {
      "Sid" : "AllowSagemakerAddTagsForAppManagedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
```

```
      "Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateSpace"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerPartnerAppsFullAccess

Descrição: permite que usuários de aplicativos SageMaker parceiros da Amazon acessem aplicativos, listem aplicativos disponíveis, iniciem interfaces de usuário web de aplicativos e se conectem por meio do SDK do aplicativo.

`AmazonSageMakerPartnerAppsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerPartnerAppsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 17 de janeiro de 2025, 18:37 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPartnerAppsFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerPartnerListAppsPermission",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListPartnerApps",
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerPartnerAppsPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePartnerAppPresignedUrl",
        "sagemaker:DescribePartnerApp",
        "sagemaker:CallPartnerAppApi"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:sagemaker:*:*:partner-app/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceR

Descrição: Política de função de serviço usada pelo AWS ApiGateway nos produtos AWS ServiceCatalog provisionados do portfólio de produtos da Amazon. SageMaker Concede permissões a um conjunto de serviços relacionados, incluindo Lambda e outros.

`AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 01 de agosto de 2023, 15:06 UTC
- Hora da edição: 01 de agosto de 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
```

```
      "Resource" : "arn:aws:lambda:*:*:function:sagemaker-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker:InvokeEndpoint",
      "Resource" : "arn:aws:sagemaker:*:*:endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServ

Descrição: Política de função de serviço usada pelo AWS CloudFormation SageMaker portfólio de produtos AWS ServiceCatalog provisionados da Amazon. Concede permissões a um subconjunto de serviços relacionados, incluindo Lambda, ApiGateway e outros.

`AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 01 de agosto de 2023, 15:06 UTC
- Hora da edição: 01 de agosto de 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsLambdaRole"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsApiGatewayRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "apigateway.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:DeleteFunction",
        "lambda:UpdateFunctionCode",
        "lambda:ListTags",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
```

```
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name",
            "sagemaker:partner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PublishLayerVersion",
        "lambda:GetLayerVersion",
        "lambda:DeleteLayerVersion",
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:layer:sagemaker-*",
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis"
      ],
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:POST",
        "apigateway:PUT"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name",
            "sagemaker:partner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/lambda-auth-code/layer.zip"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRoleP

Descrição: Política de função de serviço usada pelo AWS Lambda nos produtos AWS ServiceCatalog provisionados do SageMaker portfólio de produtos da Amazon. Concede permissões a um conjunto de serviços relacionados, incluindo Secrets Manager e outros.

`AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 01 de agosto de 2023, 15:05 UTC
- Hora da edição: 01 de agosto de 2023, 15:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:partner" : false
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerPipelinesIntegrations

Descrição: Essa política gerenciada da Amazon concede permissões normalmente necessárias para uso com etapas de retorno de chamada e etapas do Lambda em pipelines de construção de SageMaker modelos. Ele é adicionado ao AmazonSageMaker-ExecutionRole que pode ser criado ao configurar o SageMaker Studio. Também pode ser anexado a qualquer outra função que será usada para criar ou executar pipelines.

`AmazonSageMakerPipelinesIntegrations` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerPipelinesIntegrations` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de julho de 2021, 16:35 UTC
- Hora da edição: 17 de fevereiro de 2023, 21:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*sageMaker*",
        "arn:aws:lambda:*:*:function:*SageMaker*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:*sagemaker*",
        "arn:aws:sqs:*:*:*sageMaker*",
        "arn:aws:sqs:*:*:*SageMaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRStepStatusUpdateRule",
        "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRClusterStatusUpdateRule"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:RunJobFlow",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:ListSteps"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerQuickSightVPCPolicy

Descrição: Essa política será usada pela SageMaker Unified Studios para criar recursos relacionados à VPC para QuickSight

`AmazonSageMakerQuickSightVPCPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerQuickSightVPCPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 03 de junho de 2025, 17:37 UTC

- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerQuickSightVPCPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageQuickSightVPCConnection",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateVPCConnection",
        "quicksight:DescribeVPCConnection",
        "quicksight:DeleteVPCConnection",
        "quicksight:ListVPCConnections",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcconnection/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeQuickSightVPCConnectionEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageQuickSightEC2NetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerReadOnly

Descrição: Fornece acesso somente para leitura à Amazon SageMaker por meio do Console de gerenciamento da AWS SDK e.

`AmazonSageMakerReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2017, 13:07 UTC
- Hora da edição: 01 de dezembro de 2021, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sagemaker:BatchGetMetrics",
        "sagemaker:GetDeviceRegistration",
```

```
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:BatchGetRecord",
        "sagemaker:GetRecord",
        "sagemaker:Search",
        "sagemaker:QueryLineage",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:GetModelPackageGroupPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "aws-marketplace:ViewSubscriptions",
        "cloudwatch:DescribeAlarms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListUsersInGroup",
        "ecr:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePoli

Descrição: Política de função de serviço usada pelo AWS ApiGateway nos produtos AWS ServiceCatalog provisionados do portfólio de produtos da Amazon. SageMaker Concede permissões a um conjunto de serviços relacionados, incluindo CloudWatch registros e outros.

`AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 25 de março de 2022, 4:25 UTC
- Hora da edição: 25 de março de 2022, 4:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/apigateway/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerServiceCatalogProductsCloudformationServiceRoleP

Descrição: Política de função de serviço usada pelo AWS CloudFormation SageMaker portfólio de produtos AWS ServiceCatalog provisionados da Amazon. Concede permissões a um subconjunto de serviços relacionados, incluindo SageMaker e outros.

`AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 25 de março de 2022, 4:26 UTC
- Hora da edição: 25 de março de 2022, 4:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
```

```
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
```

```
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
```

```
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
```

```
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
```

```
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
```

```
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

Descrição: Política de função de serviço usada pelo AWS CodeBuild SageMaker portfólio de produtos AWS ServiceCatalog provisionados da Amazon. Concede permissões a um subconjunto de serviços relacionados CodePipeline, incluindo, CodeBuild e outros.

`AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de março de 2022, 4:27 UTC

- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildECRReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeImageReplicationStatus",
        "ecr:DescribeRepositories",
        "ecr:DescribeImageReplicationStatus",
        "ecr:GetAuthorizationToken",
```

```
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildECRWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildPassRoletPermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsEventsRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodePipelineRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "events.amazonaws.com",
            "codepipeline.amazonaws.com",
            "cloudformation.amazonaws.com",
```

```
            "codebuild.amazonaws.com",
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildLogPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*"
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
```

```
        "s3:PutBucketCors",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
```

```
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
```

```
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
```

```
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
```

```
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
```

```
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
```

```
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeStarConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeConnectionPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

Descrição: Política de função de serviço usada pelo AWS CodePipeline SageMaker portfólio de produtos AWS ServiceCatalog provisionados da Amazon. Concede permissões a um subconjunto de serviços relacionados CodePipeline, incluindo, CodeBuild e outros.

`AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 22 de fevereiro de 2022, 9:53 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerCodePipelineCFnPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCFnTagPermission",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelinePassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
```

```
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*",
        "arn:aws:codebuild:*:*:build/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeStarConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
```

```
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

Descrição: Política de função de serviço usada pelos AWS CloudWatch Eventos no SageMaker portfólio de produtos AWS ServiceCatalog provisionados da Amazon. Concede permissões a um subconjunto de serviços relacionados, incluindo CodePipeline e outros.

`AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 22 de fevereiro de 2022, 9:53 UTC
- Hora da edição: 22 de fevereiro de 2022, 9:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "codepipeline:StartPipelineExecution",
      "Resource" : "arn:aws:codepipeline:*:*:sagemaker-*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

Descrição: Política de função de serviço usada pelo AWS Firehose nos produtos AWS ServiceCatalog provisionados do SageMaker portfólio de produtos da Amazon. Concede permissões a um conjunto de serviços relacionados, incluindo Firehose e outros.

`AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 22 de fevereiro de 2022, 9:54 UTC
- Hora da edição: 22 de fevereiro de 2022, 9:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

Descrição: Política de função de serviço usada pela AWS Glue nos produtos AWS ServiceCatalog provisionados do SageMaker portfólio de produtos da Amazon. Concede permissões a um conjunto de serviços relacionados, incluindo Glue, S3 e outros.

`AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 22 de fevereiro de 2022, 9:51 UTC
- Hora da edição: 26 de agosto de 2022, 19:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetPartition",
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:DeletePartition",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:GetDatabase",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:SearchTables",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:database/sagemaker-*",
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:tableVersion/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/glue/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

Descrição: Política de função de serviço usada pelo AWS Lambda nos produtos AWS ServiceCatalog provisionados do SageMaker portfólio de produtos da Amazon. Concede permissões a um conjunto de serviços relacionados, incluindo ECR, S3 e outros.

`AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 04 de abril de 2022, 16:34 UTC
- Hora da edição: 11 de junho de 2024, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerLambdaECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeImages",
        "ecr:BatchDeleteImage",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:DeleteRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaEventBridgePermission",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
      ]
```

```
    },
    {
      "Sid" : "AmazonSageMakerLambdaS3BucketPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaS3ObjectPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
```

```
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
```

```
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
```

```
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
```

```
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
```

```
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
```

```
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:action/*",
        "arn:aws:sagemaker:*:*:algorithm/*",
        "arn:aws:sagemaker:*:*:app-image-config/*",
```

```
        "arn:aws:sagemaker:*:*:artifact/*",
        "arn:aws:sagemaker:*:*:automl-job/*",
        "arn:aws:sagemaker:*:*:code-repository/*",
        "arn:aws:sagemaker:*:*:compilation-job/*",
        "arn:aws:sagemaker:*:*:context/*",
        "arn:aws:sagemaker:*:*:data-quality-job-definition/*",
        "arn:aws:sagemaker:*:*:device-fleet/*/device/*",
        "arn:aws:sagemaker:*:*:device-fleet/*",
        "arn:aws:sagemaker:*:*:edge-packaging-job/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:experiment/*",
        "arn:aws:sagemaker:*:*:experiment-trial/*",
        "arn:aws:sagemaker:*:*:experiment-trial-component/*",
        "arn:aws:sagemaker:*:*:feature-group/*",
        "arn:aws:sagemaker:*:*:human-loop/*",
        "arn:aws:sagemaker:*:*:human-task-ui/*",
        "arn:aws:sagemaker:*:*:hyper-parameter-tuning-job/*",
        "arn:aws:sagemaker:*:*:image/*",
        "arn:aws:sagemaker:*:*:image-version/*/*",
        "arn:aws:sagemaker:*:*:inference-recommendations-job/*",
        "arn:aws:sagemaker:*:*:labeling-job/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:model-bias-job-definition/*",
        "arn:aws:sagemaker:*:*:model-explainability-job-definition/*",
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*",
        "arn:aws:sagemaker:*:*:model-quality-job-definition/*",
        "arn:aws:sagemaker:*:*:monitoring-schedule/*",
        "arn:aws:sagemaker:*:*:notebook-instance/*",
        "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:pipeline/*/execution/*",
        "arn:aws:sagemaker:*:*:processing-job/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:training-job/*",
        "arn:aws:sagemaker:*:*:transform-job/*",
        "arn:aws:sagemaker:*:*:workforce/*",
        "arn:aws:sagemaker:*:*:workteam/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaPassRolePermission",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaLogPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    },
    {
      "Sid" : "AmazonSageMakerLambdaCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:BatchGetBuilds"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/sagemaker-*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:ResourceTag/sagemaker:project-name" : "*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerSpacesControllerPolicy

Descrição: Concede ao Systems Manager as permissões de ativação, gerenciamento de sessão e operações de chaves KMS necessárias para que o complemento SageMaker Spaces permita o acesso remoto seguro aos EKS SageMaker Spaces.

`AmazonSageMakerSpacesControllerPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerSpacesControllerPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 19 de novembro de 2025, 04:34 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerSpacesControllerPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOperatorToSSMCreateActivationForSpaces",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateActivation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeActivations",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeActivations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeSessions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDeleteActivation",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteActivation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToAddTagsToActivation",
      "Effect" : "Allow",
      "Action" : "ssm:AddTagsToResource",
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:iam::*:role/sagemaker-space-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeManagedNodes",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDeregisterWorkspaceInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeregisterManagedInstance"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "ssm:resourceTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
```

```
        }
      }
    },
    {
      "Sid" : "AllowOperatorToPassSsmManagedNodeRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/sagemaker-space-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "ssm:resourceTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowStartSessionDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-StartSSHSession",
        "arn:aws:ssm:*:*:document/SageMaker-Space*"
      ]
    },
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSKeyOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:sagemaker:component" : "amazon-sagemaker-spaces",
          "kms:EncryptionContext:sagemaker:eks-cluster-arn" : "${aws:PrincipalTag/eks-
cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/SageMaker-Space*"
      ]
    },
    {
      "Sid" : "AllowOperatorToSSMCreateDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SageMaker-Space*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
```

```
        }
      }
    },
    {
      "Sid" : "AllowOperatorToEnableAdvancedTierForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting",
        "ssm:ResetServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/ssm/managed-instance/activation-
tier"
    },
    {
      "Sid" : "AllowOperatorToAddTagsToSSMDocument",
      "Effect" : "Allow",
      "Action" : "ssm:AddTagsToResource",
      "Resource" : "arn:aws:ssm:*:*:document/SageMaker-Space*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerSpacesRouterPolicy

Descrição: Concede aos sistemas as permissões de operações de chave KMS necessárias para que o SageMaker Spaces Router habilite o acesso remoto seguro aos EKS SageMaker Spaces.

`AmazonSageMakerSpacesRouterPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerSpacesRouterPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 19 de novembro de 2025, 04:34 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerSpacesRouterPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSKeyOperations",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:sagemaker:component" : "amazon-sagemaker-spaces",
          "kms:EncryptionContext:sagemaker:eks-cluster-arn" : "${aws:PrincipalTag/eks-
cluster-arn}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSageMakerTrainingPlanCreateAccess

Descrição: Essa política gerenciada da Amazon fornece as permissões necessárias para criar e gerenciar planos SageMaker de treinamento. Ela permite que os usuários criem planos de treinamento e capacidades reservadas, descrevam os planos de treinamento atuais e realizem operações de pesquisa e listagem.

`AmazonSageMakerTrainingPlanCreateAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSageMakerTrainingPlanCreateAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Horário de criação: 04 de dezembro de 2024, 13:21 UTC
- Horário editado: 12 de fevereiro de 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerTrainingPlanCreateAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingPlan",
        "sagemaker:CreateReservedCapacity",
        "sagemaker:DescribeReservedCapacity"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AddTagsToTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "sagemaker:TaggingAction" : [
            "CreateTrainingPlan",
            "CreateReservedCapacity"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeTrainingPlan",
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*"
      ]
    },
    {
      "Sid" : "NonResourceLevelTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:SearchTrainingPlanOfferings",
        "sagemaker:ListTrainingPlans"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListUltraServersByReservedCapacityPermissions",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListUltraServersByReservedCapacity",
      "Resource" : [
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSecurityLakeAdministrator

Descrição: fornece acesso total ao Amazon Security Lake e aos serviços relacionados necessários para administrar o Security Lake.

`AmazonSecurityLakeAdministrator` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSecurityLakeAdministrator` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de maio de 2023, 22:04 UTC
- Hora da edição: 23 de fevereiro de 2024, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsWithAnyResource",
      "Effect" : "Allow",
      "Action" : [
        "securitylake:*",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListAccounts",
        "iam:ListRoles",
```

```
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsWithAnyResourceViaSecurityLake",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCrawler",
        "glue:StopCrawlerSchedule",
        "lambda:CreateEventSourceMapping",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:GetDatalakeSettings",
        "events:ListConnections",
        "events:ListApiDestinations",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowManagingSecurityLakeS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketNotification",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketVersioning",
        "s3:PutReplicationConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:ListBucket",
        "s3:PutObject",
```

```
        "s3:GetBucketNotification"
      ],
      "Resource" : "arn:aws:s3:::aws-security-data-lake*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowLambdaCreateFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowLambdaAddPermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        },
        "StringEquals" : {
          "lambda:Principal" : "securitylake.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase",
        "glue:CreateTable",
        "glue:GetTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DescribeRule",
        "events:CreateApiDestination",
        "events:CreateConnection",
        "events:UpdateConnection",
        "events:UpdateApiDestination",
        "events:DeleteConnection",
        "events:DeleteApiDestination",
        "events:ListTargetsByRule",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AmazonSecurityLake*",
        "arn:aws:events:*:*:rule/SecurityLake*",
        "arn:aws:events:*:*:api-destination/AmazonSecurityLake*",
        "arn:aws:events:*:*:connection/AmazonSecurityLake*"
      ],
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSQSActions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes",
        "sqs:GetQueueURL",
        "sqs:AddPermission",
        "sqs:GetQueueAttributes",
        "sqs:DeleteQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:SecurityLake*",
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsCmkGrantForSecurityLake",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::aws-security-data-lake*"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "GenerateDataKey",
            "RetireGrant",
            "Decrypt"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AllowEnablingQueryBasedSubscribers",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare",
        "ram:AssociateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:ResourceArn" : [
            "arn:aws:glue:*:*:catalog",
            "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
            "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowConfiguringQueryBasedSubscribers",
      "Effect" : "Allow",
      "Action" : [
        "ram:UpdateResourceShare",
        "ram:GetResourceShares",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : "LakeFormation*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "AllowConfiguringCredentialsForSubscriberNotification",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/
AmazonSecurityLake-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForUpdatingGluePartitionsSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForUpdatingGluePartitionsLambdaArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        },
```

```
        "StringLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
            "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCrossRegionReplicationSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "s3.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCrossRegionReplicationS3Arn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "s3.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:s3:::aws-security-data-lake*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "AllowPassRoleForCustomSourceCrawlerSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCustomSourceCrawlerGlueArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForSubscriberNotificationSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "events.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:subscriber/*"
        }
      }
```

```
    },
    {
      "Sid" : "AllowPassRoleForSubscriberNotificationEventsArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "events.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:events:*:*:rule/AmazonSecurityLake*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowOnboardingToSecurityLakeDependencies",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/securitylake.amazonaws.com/
AWSServiceRoleForSecurityLake",
        "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
        "arn:aws:iam::*:role/aws-service-role/apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "securitylake.amazonaws.com",
            "lakeformation.amazonaws.com",
            "apidestinations.events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowRolePolicyActionsforSubscibersandSources",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonSecurityLakePermissionsBoundary"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowRegisterS3LocationInLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PutRolePolicy",
        "iam:GetRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowIAMActionsByResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRolePolicies",
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "S3ReadAccessToSecurityLakes",
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource" : "arn:aws:s3:::aws-security-data-lake-*"
    },
    {
      "Sid" : "S3ReadAccessToSecurityLakeMetastoreObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::security-lake-meta-store-manager-*"
    },
    {
      "Sid" : "S3ResourcelessReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSecurityLakeMetastoreManager

Descrição: Política para o gerenciador de SecurityLake metastores da Amazon lambda, que permite o acesso ao cloudwatch, S3, Glue e SQS.

`AmazonSecurityLakeMetastoreManager` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSecurityLakeMetastoreManager` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 23 de janeiro de 2024, 15:26 UTC
- Hora da edição: 1º de abril de 2024, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowWriteLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
```

```
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
        "arn:aws:logs:*:*:/aws/lambda/AmazonSecurityLake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowGlueManage",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToReadFromSqs",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataReadWrite",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataCleanup",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSecurityLakePermissionsBoundary

Descrição: o Amazon Security Lake cria perfis do IAM para fontes personalizadas de terceiros gravarem dados em um data lake e para que assinantes terceirizados consumam dados de um data lake e usa essa política ao criar esses perfis para definir o limite de suas permissões.

`AmazonSecurityLakePermissionsBoundary` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSecurityLakePermissionsBoundary` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2022, 14:11 UTC
- Hora da edição: 14 de maio de 2024, 20:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsForSecurityLake",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyActionsForSecurityLake",
      "Effect" : "Deny",
      "NotAction" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
```

```
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeBucket",
      "Effect" : "Deny",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "NotResource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ]
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeSQS",
      "Effect" : "Deny",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "NotResource" : "arn:aws:sqs:*:*:AmazonSecurityLake*"
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeKMSS3SQS",
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringNotLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeKMSForS3",
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringNotLikeIfExists" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::aws-security-data-lake*"
          ]
        }
      }
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeKMSForS3SQS",
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:sqs:arn" : "false"
        },
        "StringNotLikeIfExists" : {
          "kms:EncryptionContext:aws:sqs:arn" : [
            "arn:aws:sqs:*:*:AmazonSecurityLake*"
          ]
        }
```

```
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSESFullAccess

Descrição: Fornece acesso total ao Amazon SES por meio do Console de gerenciamento da AWS.

`AmazonSESFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSESFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSESReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon SES por meio do Console de gerenciamento da AWS.

`AmazonSESReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSESReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC

- Hora da edição: 14 de maio de 2024, 12:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SESReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ses:Get*",
        "ses:List*",
        "ses:BatchGetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSESServiceRolePolicy

Descrição: Permite que o SES publique métricas CloudWatch básicas de monitoramento da Amazon em nome de seus recursos do SES

`AmazonSESServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 21 de maio de 2024, 16:02 UTC
- Hora da edição: 21 de maio de 2024, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSESServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutMetricDataToSESCloudWatchNamespaces",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "AWS/SES",
            "AWS/SES/MailManager",
            "AWS/SES/Addons"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSNSFullAccess

Descrição: Fornece acesso total ao Amazon SNS por meio do Console de gerenciamento da AWS.

`AmazonSNSFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSNSFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 24 de setembro de 2024, 22:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SNSFullAccess",
      "Effect" : "Allow",
      "Action" : "sns:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SMSAccessViaSNS",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "sms-voice:CreateVerifiedDestinationNumber",
        "sms-voice:SendDestinationNumberVerificationCode",
        "sms-voice:SendTextMessage",
        "sms-voice:DeleteVerifiedDestinationNumber",
        "sms-voice:VerifyDestinationNumber",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:SetTextMessageSpendLimitOverride",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DeleteOptedOutNumber"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sns.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSNSReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon SNS por meio do Console de gerenciamento da AWS.

`AmazonSNSReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSNSReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 24 de setembro de 2024, 22:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "SNSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:List*",
        "sns:CheckIfPhoneNumberIsOptedOut",
        "sns:GetEndpointAttributes",
        "sns:GetDataProtectionPolicy",
        "sns:GetPlatformApplicationAttributes",
        "sns:GetSMSAttributes",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SMSAccessViaSNS",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribeOptedOutNumbers"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sns.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

Função do Amazon SNS

Descrição: política padrão para o perfil de serviço do Amazon SNS.

`AmazonSNSRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSNSRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSNSRole`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
```

```
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSQSFullAccess

Descrição: Fornece acesso total ao Amazon SQS por meio do Console de gerenciamento da AWS.

`AmazonSQSFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSQSFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sqs:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSQSReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon SQS por meio do Console de gerenciamento da AWS.

`AmazonSQSReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSQSReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 24 de maio de 2024, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSQSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueueTags"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSSMAutomationApproverAccess

Descrição: fornece acesso para visualizar execuções de automação e enviar decisões de aprovação para a automação que aguardam aprovação

`AmazonSSMAutomationApproverAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSSMAutomationApproverAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 07 de agosto de 2017, 23:07 UTC
- Hora da edição: 07 de agosto de 2017, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:GetAutomationExecution",
        "ssm:SendAutomationSignal"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSSMAutomationRole

Descrição: fornece permissões para o serviço de automação do EC2 executar atividades definidas nos documentos de automação

`AmazonSSMAutomationRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSSMAutomationRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 05 de dezembro de 2016, 22:09 UTC
- Horário editado: 20 de março de 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:Automation*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
        "ec2:DeleteSnapshot",
        "ec2:StartInstances",
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
```

```
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:Automation*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:*:ssm:*:*:session/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSSMDirectoryServiceAccess

Descrição: esta política permite que o SSM Agent acesse o Directory Service em nome do cliente para ingressar no domínio da instância gerenciada.

`AmazonSSMDirectoryServiceAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSSMDirectoryServiceAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de março de 2019, 17:44 UTC
- Hora da edição: 15 de março de 2019, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ds:DescribeDirectories"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSSMFullAccess

Descrição: fornece acesso total ao Amazon SSM.

`AmazonSSMFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSSMFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de maio de 2015, 17:39 UTC
- Hora da edição: 20 de novembro de 2019, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeInstanceStatus",
        "logs:*",
        "ssm:*",
        "ec2messages:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
```

```
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSSMMaintenanceWindowRole

Descrição: perfil de serviço a ser usado na janela de manutenção do EC2

`AmazonSSMMaintenanceWindowRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSSMMaintenanceWindowRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 01 de dezembro de 2016, 15:57 UTC
- Hora da edição: 27 de julho de 2019, 0:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "states:DescribeExecution",
        "states:StartExecution"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:SSM*",
        "arn:aws:states:*:*:execution:SSM*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSSMManagedEC2InstanceDefaultPolicy

Descrição: Essa política ativa a funcionalidade do AWS Systems Manager em instâncias do EC2.

`AmazonSSMManagedEC2InstanceDefaultPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSSMManagedEC2InstanceDefaultPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de agosto de 2022, 20:54 UTC
- Hora da edição: 16 de julho de 2024, 18:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMAgentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowSSMChannelMessaging",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSSMLegacyMessaging",
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSSMManagedInstanceCore

Descrição: A política do Amazon EC2 Role para habilitar a funcionalidade principal do serviço do AWS Systems Manager.

`AmazonSSMManagedInstanceCore` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSSMManagedInstanceCore` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de março de 2019, 17:22 UTC
- Hora da edição: 23 de maio de 2019, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
```

```
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSSMPatchAssociation

Descrição: fornece acesso a instâncias filhas para operações de associação de patches.

`AmazonSSMPatchAssociation` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSSMPatchAssociation` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 13 de maio de 2020, 16:00 UTC
- Hora da edição: 13 de maio de 2020, 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMPatchAssociation`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ssm:DescribeEffectivePatchesForPatchBaseline",
      "Resource" : "arn:aws:ssm:*:*:patchbaseline/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:GetPatchBaseline",
      "Resource" : "arn:aws:ssm:*:*:patchbaseline/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:DescribePatchBaselines",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSSMReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon SSM.

`AmazonSSMReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSSMReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de maio de 2015, 17:44 UTC
- Hora da edição: 29 de maio de 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSSMServiceRolePolicy

Descrição: Fornece acesso aos AWS recursos gerenciados ou usados pelo Amazon SSM

`AmazonSSMServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 13 de novembro de 2017, 19:20 UTC
- Horário editado: 26 de junho de 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy`

Versão da política

Versão da política: v17 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListTagsForResource",
        "ssm:GetCalendarState",
        "ssm:ListCloudConnectors"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutInventory"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "ssm:InventoryTypeName" : [
            "AWS:ComplianceItem",
            "AWS:PatchSummary"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
```

```
      "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "states:DescribeExecution",
        "states:StartExecution"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:SSM*",
        "arn:aws:states:*:*:execution:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:SelectResourceConfig"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEnrollmentStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeCases"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeComplianceByResource",
        "config:DescribeRemediationConfigurations",
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:ListStackSets",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackInstances",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:DeleteStackSet"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:DeleteStackInstances",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*",
        "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-SSM*:*",
        "arn:aws:cloudformation:*:*:type/resource/*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/SSMExplorerManagedRule"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "events:DescribeRule",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "securityhub:DescribeHub",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-explorer-2:CreateManagedView",
      "Resource" : "arn:aws:resource-explorer-2:*:*:managed-view/AWSManagedViewForSSM*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonSumerianFullAccess

Descrição: fornece acesso total ao Amazon Sumerian.

`AmazonSumerianFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonSumerianFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de abril de 2018, 20:14 UTC
- Hora da edição: 24 de abril de 2018, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSumerianFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "sumerian:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonTextractFullAccess

Descrição: acesso a todas as APIs do Amazon Textract

`AmazonTextractFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonTextractFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2018, 19:07 UTC
- Hora da edição: 28 de novembro de 2018, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTextractFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "textract:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonTextractServiceRole

Descrição: Permite que o Textract ligue para AWS os serviços em seu nome.

`AmazonTextractServiceRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonTextractServiceRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 28 de novembro de 2018, 19:12 UTC
- Hora da edição: 28 de novembro de 2018, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:AmazonTextract*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonTimestreamConsoleFullAccess

Descrição: fornece acesso total para gerenciar o Amazon Timestream usando o Console de gerenciamento da AWS. Observe que essa política também concede permissões para determinadas operações do KMS e operações para gerenciar suas consultas salvas. Se estiver usando a CMK gerenciada pelo cliente, consulte a documentação para obter as permissões adicionais necessárias.

`AmazonTimestreamConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonTimestreamConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de setembro de 2020, 21:47 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess`

Versão da política

Versão da política: v13 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dbqms:CreateFavoriteQuery",
        "dbqms:DescribeFavoriteQueries",
        "dbqms:UpdateFavoriteQuery",
        "dbqms:DeleteFavoriteQueries",
        "dbqms:GetQueryString",
        "dbqms:CreateQueryHistory",
        "dbqms:DescribeQueryHistory",
        "dbqms:UpdateQueryHistory",
        "dbqms:DeleteQueryHistory"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:ListEntitlementDetails",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:Subscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "prod-xcc5llpq4vlbc",
            "prod-5jijo74ujy36m",
```

```
            "prod-rjppt7huo35fm"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonTimestreamFullAccess

Descrição: fornece acesso total ao Amazon Timestream. Observe que essa política também concede acesso a determinadas operações do KMS. Se estiver usando a CMK gerenciada pelo cliente, consulte a documentação para obter as permissões adicionais necessárias.

`AmazonTimestreamFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonTimestreamFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de setembro de 2020, 21:47 UTC
- Hora da edição: 26 de novembro de 2021, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonTimestreamInfluxDBFullAccess

Descrição: fornece acesso administrativo total para criar, atualizar, excluir e listar instâncias do Amazon Timestream InfluxDB e criar e listar grupos de parâmetros. Consulte a documentação para ver quais são as permissões adicionais necessárias.

`AmazonTimestreamInfluxDBFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonTimestreamInfluxDBFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de março de 2024, 22:53 UTC
- Horário editado: 03 de agosto de 2026, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess`

Versão da política

Versão da política: v18 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TimestreamInfluxDBStatement",
      "Effect" : "Allow",
      "Action" : [
        "timestream-influxdb:CreateDbParameterGroup",
        "timestream-influxdb:GetDbParameterGroup",
        "timestream-influxdb:ListDbParameterGroups",
        "timestream-influxdb:CreateDbInstance",
        "timestream-influxdb:DeleteDbInstance",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:TagResource",
        "timestream-influxdb:UntagResource",
        "timestream-influxdb:ListTagsForResource",
        "timestream-influxdb:UpdateDbInstance",
        "timestream-influxdb:CreateDbCluster",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:UpdateDbCluster",
        "timestream-influxdb:DeleteDbCluster",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstancesForCluster",
        "timestream-influxdb:RebootDbInstance",
        "timestream-influxdb:RebootDbCluster",
        "timestream-influxdb:CreateDbBackup",
        "timestream-influxdb:GetDbBackup",
        "timestream-influxdb:ListDbBackups",
        "timestream-influxdb:DeleteDbBackup",
        "timestream-influxdb:RestoreFromDbBackup"
      ],
      "Resource" : "arn:aws:timestream-influxdb:*:*:*"
```

```
    },
    {
      "Sid" : "ServiceLinkedRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/timestream-
influxdb.amazonaws.com/AWSServiceRoleForTimestreamInfluxDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "timestream-influxdb.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BucketValidationStatement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid" : "MPViewAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MPSubscriptionAccessStatement",
      "Effect" : "Allow",
      "Action" : "aws-marketplace:Subscribe",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "prod-xcc5llpq4vlbc",
            "prod-rjppt7huo35fm"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess

Descrição: concede acesso administrativo para gerenciar instâncias e grupos de parâmetros do Amazon Timestream InfluxDB, exceto operações de mercado.

`AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 17 de abril de 2025, 17:52 UTC
- Horário editado: 03 de agosto de 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TimestreamInfluxDBStatement",
      "Effect" : "Allow",
      "Action" : [
        "timestream-influxdb:CreateDbParameterGroup",
```

```
        "timestream-influxdb:GetDbParameterGroup",
        "timestream-influxdb:ListDbParameterGroups",
        "timestream-influxdb:CreateDbInstance",
        "timestream-influxdb:DeleteDbInstance",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:TagResource",
        "timestream-influxdb:UntagResource",
        "timestream-influxdb:ListTagsForResource",
        "timestream-influxdb:UpdateDbInstance",
        "timestream-influxdb:CreateDbCluster",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:UpdateDbCluster",
        "timestream-influxdb:DeleteDbCluster",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstancesForCluster",
        "timestream-influxdb:RebootDbInstance",
        "timestream-influxdb:RebootDbCluster",
        "timestream-influxdb:CreateDbBackup",
        "timestream-influxdb:GetDbBackup",
        "timestream-influxdb:ListDbBackups",
        "timestream-influxdb:DeleteDbBackup",
        "timestream-influxdb:RestoreFromDbBackup"
      ],
      "Resource" : [
        "arn:aws:timestream-influxdb:*:*:*"
      ]
    },
    {
      "Sid" : "ServiceLinkedRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/timestream-
influxdb.amazonaws.com/AWSServiceRoleForTimestreamInfluxDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "timestream-influxdb.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkValidationStatement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BucketValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonTimestreamInfluxDBServiceRolePolicy

Descrição: fornece acesso administrativo total para criar, atualizar, excluir e listar instâncias do Amazon Timestream InfluxDB e criar e listar grupos de parâmetros. Consulte a documentação para ver quais são as permissões adicionais necessárias.

`AmazonTimestreamInfluxDBServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 14 de março de 2024, 18:53 UTC
- Horário editado: 20 de julho de 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "CreateEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CreateTagWithEniStatement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "ManageEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonTimestreamInfluxDBManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PutCloudWatchMetricsStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Timestream/InfluxDB",
            "AWS/Usage"
          ]
        }
      },
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "ManageSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:READONLY-InfluxDB-auth-parameters-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RetrievePluginSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:InfluxDB-RepoToken-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DecryptPluginSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:*:kms:*:${aws:PrincipalAccount}:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" :
 "arn:*:secretsmanager:*:*:secret:InfluxDB-RepoToken-*"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonTimestreamReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon Timestream. A política também fornece permissão para cancelar qualquer consulta em execução. Se estiver usando a CMK gerenciada pelo cliente, consulte a documentação para obter as permissões adicionais necessárias.

`AmazonTimestreamReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonTimestreamReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de setembro de 2020, 21:47 UTC
- Hora da edição: 5 de junho de 2024, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonTimestreamReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:CancelQuery",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:Select",
        "timestream:SelectValues",
        "timestream:DescribeScheduledQuery",
        "timestream:ListScheduledQueries",
        "timestream:DescribeBatchLoadTask",
        "timestream:ListBatchLoadTasks",
        "timestream:DescribeAccountSettings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonTranscribeFullAccess

Descrição: fornece acesso total a operações do Amazon Transcribe.

`AmazonTranscribeFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonTranscribeFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 04 de abril de 2018, 16:06 UTC
- Hora da edição: 04 de abril de 2018, 16:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*transcribe*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonTranscribeReadOnlyAccess

Descrição: fornece acesso somente leitura para operação do Amazon Transcribe.

`AmazonTranscribeReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonTranscribeReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 04 de abril de 2018, 16:05 UTC
- Hora da edição: 04 de abril de 2018, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:Get*",
        "transcribe:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonVerifiedPermissionsFullAccess

Descrição: fornece acesso total ao Verified Permissions

`AmazonVerifiedPermissionsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonVerifiedPermissionsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de outubro de 2024, 18:19 UTC
- Hora da edição: 11 de outubro de 2024, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVerifiedPermissionsFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccountLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:CreatePolicyStore",
        "verifiedpermissions:ListPolicyStores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PolicyStoreLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:*"
      ],
      "Resource" : [
        "arn:aws:verifiedpermissions::*:policy-store/*"
      ]
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonVerifiedPermissionsReadOnlyAccess

Descrição: fornece acesso somente leitura ao serviço Verified Permissions.

`AmazonVerifiedPermissionsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonVerifiedPermissionsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de outubro de 2024, 18:25 UTC
- Hora da edição: 11 de outubro de 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVerifiedPermissionsReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccountLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:ListPolicyStores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PolicyStoreLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:IsAuthorized",
        "verifiedpermissions:IsAuthorizedWithToken",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyTemplates"
      ],
      "Resource" : [
        "arn:aws:verifiedpermissions::*:policy-store/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonVPCCrossAccountNetworkInterfaceOperations

Descrição: permite criar interfaces de rede e as anexar a recursos entre contas

`AmazonVPCCrossAccountNetworkInterfaceOperations` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonVPCCrossAccountNetworkInterfaceOperations` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de julho de 2017, 20:47 UTC
- Hora da edição: 25 de setembro de 2023, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:ReplaceRoute"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : [
        "*"
      ]
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonVPCFullAccess

Descrição: Fornece acesso total ao Amazon VPC por meio do Console de gerenciamento da AWS.

`AmazonVPCFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonVPCFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

Versão da política

Versão da política: v13 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSecurityGroupVpc",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCarrierGateway",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateFlowLogs",
        "ec2:CreateInternetGateway",
        "ec2:CreateLocalGatewayRouteTableVpcAssociation",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
```

```
            "ec2:CreateSubnet",
            "ec2:CreateTags",
            "ec2:CreateVpc",
            "ec2:CreateVpcEndpoint",
            "ec2:CreateVpcEndpointConnectionNotification",
            "ec2:CreateVpcEndpointServiceConfiguration",
            "ec2:CreateVpcPeeringConnection",
            "ec2:CreateVpnConnection",
            "ec2:CreateVpnConnectionRoute",
            "ec2:CreateVpnGateway",
            "ec2:DeleteCarrierGateway",
            "ec2:DeleteCustomerGateway",
            "ec2:DeleteDhcpOptions",
            "ec2:DeleteEgressOnlyInternetGateway",
            "ec2:DeleteFlowLogs",
            "ec2:DeleteInternetGateway",
            "ec2:DeleteLocalGatewayRouteTableVpcAssociation",
            "ec2:DeleteNatGateway",
            "ec2:DeleteNetworkAcl",
            "ec2:DeleteNetworkAclEntry",
            "ec2:DeleteNetworkInterface",
            "ec2:DeleteNetworkInterfacePermission",
            "ec2:DeleteRoute",
            "ec2:DeleteRouteTable",
            "ec2:DeleteSecurityGroup",
            "ec2:DeleteSubnet",
            "ec2:DeleteTags",
            "ec2:DeleteVpc",
            "ec2:DeleteVpcEndpoints",
            "ec2:DeleteVpcEndpointConnectionNotifications",
            "ec2:DeleteVpcEndpointServiceConfigurations",
            "ec2:DeleteVpcPeeringConnection",
            "ec2:DeleteVpnConnection",
            "ec2:DeleteVpnConnectionRoute",
            "ec2:DeleteVpnGateway",
            "ec2:DescribeAccountAttributes",
            "ec2:DescribeAddresses",
            "ec2:DescribeAvailabilityZones",
            "ec2:DescribeCarrierGateways",
            "ec2:DescribeClassicLinkInstances",
            "ec2:DescribeCustomerGateways",
            "ec2:DescribeDhcpOptions",
            "ec2:DescribeEgressOnlyInternetGateways",
            "ec2:DescribeFlowLogs",
```

```
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DetachClassicLinkVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLink",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSecurityGroupVpc",
```

```
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVpcClassicLink",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySecurityGroupRules",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ModifyVpcEndpointConnectionNotification",
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:ModifyVpcPeeringConnectionOptions",
        "ec2:ModifyVpcTenancy",
        "ec2:MoveAddressToVpc",
        "ec2:RejectVpcEndpointConnections",
        "ec2:RejectVpcPeeringConnection",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:ResetNetworkInterfaceAttribute",
        "ec2:RestoreAddressToClassic",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

Descrição: fornece permissões para descrever AWS recursos, executar o Network Access Analyzer e criar ou excluir tags no Network Insights Access Scope e Network Insights Access Scope Analysis.

`AmazonVPCNetworkAccessAnalyzerFullAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonVPCNetworkAccessAnalyzerFullAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de junho de 2023, 22:56 UTC
- Horário editado: 14 de agosto de 2026, 17:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectconnectPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsAccessScope",
        "ec2:DeleteNetworkInsightsAccessScope",
        "ec2:DeleteNetworkInsightsAccessScopeAnalysis",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:GetTransitGatewayPolicyTableEntries",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
```

```
        "ec2:DescribeAddresses",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAccessScopeAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-insights-access-scope/*",
        "arn:*:ec2:*:*:network-insights-access-scope-analysis/*"
      ]
    },
    {
      "Sid" : "ElasticloadbalancingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlobalacceleratorPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallMetadata",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TirosPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonVPCReachabilityAnalyzerFullAccessPolicy

Descrição: fornece permissões para descrever AWS recursos, executar o Acchability Analyzer e criar ou excluir tags no Network Insights Path e Network Insights Analysis.

`AmazonVPCReachabilityAnalyzerFullAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonVPCReachabilityAnalyzerFullAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de junho de 2023, 20:12 UTC
- Horário editado: 14 de agosto de 2026, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectconnectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:GetTransitGatewayPolicyTableEntries",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeAddresses",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-insights-path/*",
        "arn:*:ec2:*:*:network-insights-analysis/*"
      ]
    },
    {
      "Sid" : "ElasticloadbalancingPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlobalacceleratorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallMetadata",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TirosPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

Descrição: Essa política está anexada à função IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess. Essa função é implantada nas contas dos membros em uma organização quando a conta de gerenciamento permite acesso confiável ao Reachability Analyzer. Ele fornece permissões para visualizar recursos de toda a organização usando o console do Reachability Analyzer.

`AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de maio de 2023, 20:38 UTC

- Hora da edição: 01 de maio de 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:Describe*",
        "network-firewall:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonVPCReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon VPC por meio do Console de gerenciamento da AWS.

`AmazonVPCReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonVPCReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
```

```
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkDocsFullAccess

Descrição: Fornece acesso total à Amazon WorkDocs por meio do Console de gerenciamento da AWS

`AmazonWorkDocsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonWorkDocsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 16 de abril de 2020, 23:05 UTC
- Hora da edição: 16 de abril de 2020, 23:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkDocsReadOnlyAccess

Descrição: Fornece acesso somente para leitura à Amazon WorkDocs por meio do Console de gerenciamento da AWS

`AmazonWorkDocsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonWorkDocsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de janeiro de 2020, 23:49 UTC
- Hora da edição: 08 de janeiro de 2020, 23:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkMailEventsServiceRolePolicy

Descrição: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pela Amazon WorkMail Events

`AmazonWorkMailEventsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 16 de abril de 2019, 16:52 UTC
- Hora da edição: 16 de abril de 2019, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkMailFullAccess

Descrição: Fornece acesso total ao Directory Service WorkMail, SES, EC2 e acesso de leitura aos metadados do KMS.

`AmazonWorkMailFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonWorkMailFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 21 de dezembro de 2020, 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailFullAccess`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:CheckAlias",
        "ds:CreateAlias",
        "ds:CreateDirectory",
        "ds:CreateIdentityPoolDirectory",
        "ds:DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:ListAuthorizedApplications",
        "ds:UnauthorizeApplication",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "route53:ChangeResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53:GetHostedZone",
        "route53domains:CheckDomainAvailability",
        "route53domains:ListDomains",
        "ses:*",
        "workmail:*",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "cloudwatch:GetMetricData"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "events.workmail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.workmail.amazonaws.com/
AWSServiceRoleForAmazonWorkMailEvents*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*workmail*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "events.workmail.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkMailMessageFlowFullAccess

Descrição: Acesso total às APIs do fluxo de WorkMail mensagens

`AmazonWorkMailMessageFlowFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonWorkMailMessageFlowFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de fevereiro de 2021, 11:08 UTC
- Hora da edição: 11 de fevereiro de 2021, 11:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workmailmessageflow:*"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkMailMessageFlowReadOnlyAccess

Descrição: acesso somente para leitura às WorkMail mensagens da GetRawMessageContent API

`AmazonWorkMailMessageFlowReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonWorkMailMessageFlowReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de janeiro de 2021, 12:40 UTC
- Hora da edição: 28 de janeiro de 2021, 12:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "workmailmessageflow:Get*"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkMailReadOnlyAccess

Descrição: Fornece acesso somente para leitura WorkMail e SES.

`AmazonWorkMailReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonWorkMailReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 25 de julho de 2019, 8:24 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:Describe*",
        "ses:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "lambda:ListFunctions",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkSpacesAdmin

Descrição: Fornece acesso às ações WorkSpaces administrativas da Amazon por meio do AWS SDK e da CLI.

`AmazonWorkSpacesAdmin` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonWorkSpacesAdmin` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 22 de setembro de 2015, 22:21 UTC
- Hora da edição: 27 de junho de 2024, 17:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonWorkSpacesAdmin",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "workspaces:CreateTags",
```

```
        "workspaces:CreateWorkspaceImage",
        "workspaces:CreateWorkspaces",
        "workspaces:CreateWorkspacesPool",
        "workspaces:CreateStandbyWorkspaces",
        "workspaces:DeleteTags",
        "workspaces:DeregisterWorkspaceDirectory",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspacesPools",
        "workspaces:DescribeWorkspacesPoolSessions",
        "workspaces:DescribeWorkspacesConnectionStatus",
        "workspaces:ModifyCertificateBasedAuthProperties",
        "workspaces:ModifySamlProperties",
        "workspaces:ModifyStreamingProperties",
        "workspaces:ModifyWorkspaceCreationProperties",
        "workspaces:ModifyWorkspaceProperties",
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:RegisterWorkspaceDirectory",
        "workspaces:RestoreWorkspace",
        "workspaces:StartWorkspaces",
        "workspaces:StartWorkspacesPool",
        "workspaces:StopWorkspaces",
        "workspaces:StopWorkspacesPool",
        "workspaces:TerminateWorkspaces",
        "workspaces:TerminateWorkspacesPool",
        "workspaces:TerminateWorkspacesPoolSession",
        "workspaces:UpdateWorkspacesPool"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkSpacesApplicationManagerAdminAccess

Descrição: Fornece acesso de administrador para empacotar um aplicativo no Amazon WorkSpaces Application Manager.

`AmazonWorkSpacesApplicationManagerAdminAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonWorkSpacesApplicationManagerAdminAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de abril de 2015, 14:03 UTC
- Hora da edição: 09 de abril de 2015, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wam:AuthenticatePackager",
      "Resource" : "*"
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkspacesPCAAccess

Descrição: Essa política gerenciada fornece acesso administrativo total aos recursos de CA privada do AWS Certificate Manager Conta da AWS para autenticação baseada em certificados.

`AmazonWorkspacesPCAAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonWorkspacesPCAAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de novembro de 2022, 0:25 UTC
- Hora da edição: 08 de novembro de 2022, 0:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:*:acm-pca:*:*:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/euc-private-ca" : "*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkSpacesPoolServiceAccess

Descrição: Essa política fornece acesso de AWS WorkSpaces serviço aos recursos necessários da conta do cliente para o lançamento de Workspaces Pools

`AmazonWorkSpacesPoolServiceAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonWorkSpacesPoolServiceAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de junho de 2024, 16:21 UTC
- Hora da edição: 27 de junho de 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesPoolServiceAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProvisioningWorkSpacesPoolPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "WorkSpacesPoolS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::wspool-logs-*",
        "arn:aws:s3:::wspool-app-settings-*",
        "arn:aws:s3:::wspool-home-folder-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkSpacesSecureBrowserReadOnly

Descrição: Fornece acesso somente para leitura ao Amazon WorkSpaces Secure Browser e suas dependências por meio do SDK e da Console de gerenciamento da AWS CLI.

`AmazonWorkSpacesSecureBrowserReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonWorkSpacesSecureBrowserReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de junho de 2024, 20:01 UTC
- Hora da edição: 24 de junho de 2024, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSecureBrowserReadOnly`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkSpacesSecureBrowser",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetBrowserSettings",
```

```
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserSettings",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetIpAccessSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserSettings",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListIpAccessSettings"
      ],
      "Resource" : "arn:aws:workspaces-web:*:*:*"
    },
    {
      "Sid" : "Dependencies",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkSpacesSelfServiceAccess

Descrição: Fornece acesso ao serviço de WorkSpaces back-end da Amazon para realizar ações de autoatendimento do Workspace

`AmazonWorkSpacesSelfServiceAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonWorkSpacesSelfServiceAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de junho de 2019, 19:22 UTC
- Hora da edição: 27 de junho de 2019, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:ModifyWorkspaceProperties"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkSpacesServiceAccess

Descrição: Fornece acesso à conta do cliente ao AWS WorkSpaces serviço para lançar um espaço de trabalho.

`AmazonWorkSpacesServiceAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonWorkSpacesServiceAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de junho de 2019, 19:19 UTC
- Hora da edição: 18 de março de 2020, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkSpacesThinClientFullAccess

Descrição: Fornece acesso total ao Amazon WorkSpaces Thin Client, bem como acesso limitado aos serviços relacionados necessários

`AmazonWorkSpacesThinClientFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonWorkSpacesThinClientFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 9 de agosto de 2024, 7:25 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientFullAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowThinClientFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "thinclient:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesSecureBrowserAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "appstream:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
monitoring.thinclient.amazonaws.com/
AWSServiceRoleForAmazonWorkSpacesThinClientMonitoring",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "monitoring.thinclient.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkSpacesThinClientMonitoringServiceRolePolicy

Descrição: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo Amazon WorkSpaces Thin Client Monitoring

`AmazonWorkSpacesThinClientMonitoringServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 13 de junho de 2025, 19:37 UTC
- Horário editado: 13 de junho de 2025, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesThinClientMonitoringServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudWatchPutMetricData",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "cloudwatch:namespace" : [
            "AWS/WorkSpacesThinClient",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkSpacesThinClientReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon WorkSpaces Thin Client e suas dependências

`AmazonWorkSpacesThinClientReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonWorkSpacesThinClientReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 19 de julho de 2024, 8:50 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientReadOnlyAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowThinClientReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "thinclient:GetDevice",
        "thinclient:GetDeviceDetails",
        "thinclient:GetEnvironment",
        "thinclient:GetSoftwareSet",
        "thinclient:ListDevices",
        "thinclient:ListDeviceSessions",
        "thinclient:ListEnvironments",
        "thinclient:ListSoftwareSets",
        "thinclient:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesSecureBrowserAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowAppStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "appstream:DescribeStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkSpacesWebReadOnly

Descrição: Fornece acesso somente para leitura à Amazon WorkSpaces Web e suas dependências por meio do SDK e da Console de gerenciamento da AWS CLI.

`AmazonWorkSpacesWebReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonWorkSpacesWebReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de novembro de 2021, 14:20 UTC
- Hora da edição: 02 de novembro de 2022, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserSettings",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserSettings",
        "workspaces-web:ListUserAccessLoggingSettings"
      ],
      "Resource" : "arn:aws:workspaces-web:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
```

```
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonWorkSpacesWebServiceRolePolicy

Descrição: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pela Amazon WorkSpaces Web

`AmazonWorkSpacesWebServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 30 de novembro de 2021, 13:15 UTC
- Hora da edição: 15 de dezembro de 2022, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/WorkSpacesWebManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "WorkSpacesWebManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/WorkSpacesWebManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "cloudwatch:namespace" : [
            "AWS/WorkSpacesWeb",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStreamSummary"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/amazon-workspaces-web-*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonZocaloFullAccess

Descrição: fornece acesso total ao Amazon Zocalo.

`AmazonZocaloFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonZocaloFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:*",
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmazonZocaloReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon Zocalo

`AmazonZocaloReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmazonZocaloReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:Describe*",
```

```
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AmplifyBackendDeployFullAccess

Descrição: Fornece permissões de acesso total ao Amplify para implantar recursos de back-end do Amplify (Amazon Cognito AWS AppSync, Amazon S3 e outros serviços relacionados) por meio do Nuvem AWS Kit de Desenvolvimento (CDK)AWS

`AmplifyBackendDeployFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AmplifyBackendDeployFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 06 de outubro de 2023, 21:32 UTC
- Horário editado: 14 de novembro de 2024, 19:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CDKPreDeploy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*",
        "arn:aws:cloudformation:*:*:stack/CDKToolkit/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyMetadata",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "cloudformation:ListStacks",
        "ssm:DescribeParameters",
        "appsync:GetIntrospectionSchema",
        "amplify:GetBackendEnvironment"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "AmplifyHotSwappableResources",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetSchemaCreationStatus",
        "appsync:StartSchemaCreation",
        "appsync:UpdateResolver",
        "appsync:ListFunctions",
        "appsync:UpdateFunction",
        "appsync:UpdateApiKey"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableFunctionResource",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:amplify-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifySandboxLambdaLogsStreamingListTags",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListTags"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:amplify-*"
      ]
    },
```

```
    {
      "Sid" : "AmplifySandboxLambdaLogsStreamingFilterLogEvents",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/amplify-*:*",
        "arn:aws:logs:*:*:log-group:amplify-*:*"
      ]
    },
    {
      "Sid" : "AmplifySchema",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*amplify*",
        "arn:aws:s3:::cdk-*-assets-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CDKDeploy",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cdk-*-deploy-role-*-*",
        "arn:aws:iam::*:role/cdk-*-file-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-image-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-lookup-role-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "AmplifySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath",
        "ssm:GetParameters",
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amplify/*",
        "arn:aws:ssm:*:*:parameter/cdk-bootstrap/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyModifySSMParam",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:DeleteParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyDiscoverRDSVpcConfig",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBProxies",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "ec2:DescribeSubnets",
        "rds:DescribeDBSubnetGroups"
      ],
```

```
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:db-proxy:*",
        "arn:aws:rds:*:*:subgrp:*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AnthropicFullAccess

Descrição: Fornece acesso total à Plataforma Claude em AWS

`AnthropicFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AnthropicFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 01 de abril de 2026, 04:57 UTC
- Horário editado: 25 de setembro de 2026, 20:17 UTC
- ARN: `arn:aws:iam::aws:policy/AnthropicFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AnthropicFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicSubscriptionManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "prod-3qbeiztufnva6"
          ]
        }
      }
    },
    {
      "Sid" : "AnthropicSubscriptionView",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicFullEnableFederation",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetOutboundWebIdentityFederationInfo",
        "iam:EnableOutboundWebIdentityFederation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicFullGetToken",
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "sts:IdentityTokenAudience" : [
            "https://api.anthropic.com",
            "https://platform.claude.com"
          ]
        },
        "StringEquals" : {
          "aws:CalledViaLast" : "aws-external-anthropic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AnthropicFullTagToken",
      "Effect" : "Allow",
      "Action" : "sts:TagGetWebIdentityToken",
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicReadOnlyKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AnthropicLimitedAccess

Descrição: Fornece acesso limitado à Plataforma Claude em AWS

`AnthropicLimitedAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AnthropicLimitedAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 01 de abril de 2026, 04:57 UTC
- Horário editado: 02 de outubro de 2026, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AnthropicLimitedAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AnthropicLimitedWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:Get*",
        "aws-external-anthropic:List*",
        "aws-external-anthropic:ArchiveAgent",
        "aws-external-anthropic:ArchiveEnvironment",
        "aws-external-anthropic:ArchiveMemoryStore",
        "aws-external-anthropic:ArchiveSession",
        "aws-external-anthropic:ArchiveVault",
        "aws-external-anthropic:CancelBatchInference",
        "aws-external-anthropic:CountTokens",
        "aws-external-anthropic:CreateAgent",
        "aws-external-anthropic:CreateBatchInference",
        "aws-external-anthropic:CreateEnvironment",
        "aws-external-anthropic:CreateFile",
        "aws-external-anthropic:CreateInference",
        "aws-external-anthropic:CreateMemoryStore",
        "aws-external-anthropic:CreateSession",
        "aws-external-anthropic:CreateSkill",
        "aws-external-anthropic:CreateVault",
        "aws-external-anthropic:CreateWebhook",
        "aws-external-anthropic:DeleteBatchInference",
        "aws-external-anthropic:DeleteEnvironment",
        "aws-external-anthropic:DeleteFile",
        "aws-external-anthropic:DeleteMemoryStore",
        "aws-external-anthropic:DeleteSession",
        "aws-external-anthropic:DeleteSkill",
        "aws-external-anthropic:DeleteVault",
        "aws-external-anthropic:DeleteWebhook",
        "aws-external-anthropic:ProcessEnvironmentWork",
        "aws-external-anthropic:RotateWebhookSecret",
        "aws-external-anthropic:UpdateAgent",
        "aws-external-anthropic:UpdateEnvironment",
        "aws-external-anthropic:UpdateMemoryStore",
        "aws-external-anthropic:UpdateSession",
        "aws-external-anthropic:UpdateSkill",
        "aws-external-anthropic:UpdateVault",
        "aws-external-anthropic:UpdateWebhook"
      ],
      "Resource" : "arn:aws:aws-external-anthropic:*:*:workspace/*"
```

```
    },
    {
      "Sid" : "AnthropicLimitedResourceless",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:GetAccountStatus",
        "aws-external-anthropic:CallWithBearerToken",
        "aws-external-anthropic:ListKeys",
        "aws-external-anthropic:GetKey",
        "aws-external-anthropic:CreateUserProfile",
        "aws-external-anthropic:GetUserProfile",
        "aws-external-anthropic:UpdateUserProfile",
        "aws-external-anthropic:ListUserProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicLimitedGetToken",
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "sts:IdentityTokenAudience" : [
            "https://api.anthropic.com",
            "https://platform.claude.com"
          ]
        },
        "StringEquals" : {
          "aws:CalledViaLast" : "aws-external-anthropic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AnthropicLimitedTagToken",
      "Effect" : "Allow",
      "Action" : "sts:TagGetWebIdentityToken",
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicLimitedConsoleAccess",
      "Effect" : "Allow",
      "Action" : "aws-external-anthropic:AssumeConsole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws-external-anthropic:Capability" : "developer"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AnthropicReadOnlyAccess

Descrição: Fornece acesso somente para leitura à Plataforma Claude em AWS

`AnthropicReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AnthropicReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 01 de abril de 2026, 04:57 UTC
- Horário editado: 02 de outubro de 2026, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AnthropicReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AnthropicReadOnlyWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:Get*",
        "aws-external-anthropic:List*"
      ],
      "Resource" : "arn:aws:aws-external-anthropic:*:*:workspace/*"
    },
    {
      "Sid" : "AnthropicReadOnlyResourceless",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:GetAccountStatus",
        "aws-external-anthropic:CallWithBearerToken",
        "aws-external-anthropic:ListKeys",
        "aws-external-anthropic:GetKey",
        "aws-external-anthropic:GetUserProfile",
        "aws-external-anthropic:ListUserProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicReadOnlyKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AnthropicReadOnlyGetToken",
      "Effect" : "Allow",
```

```
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "sts:IdentityTokenAudience" : [
            "https://api.anthropic.com",
            "https://platform.claude.com"
          ]
        },
        "StringEquals" : {
          "aws:CalledViaLast" : "aws-external-anthropic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AnthropicReadOnlyTagToken",
      "Effect" : "Allow",
      "Action" : "sts:TagGetWebIdentityToken",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AnthropicSelfHostedEnvironmentAccess

Descrição: Fornece acesso para operar um executor de ambiente auto-hospedado para Claude Managed Agents

`AnthropicSelfHostedEnvironmentAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AnthropicSelfHostedEnvironmentAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 12 de junho de 2026, 17:12 UTC
- Horário editado: 12 de junho de 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AnthropicSelfHostedEnvironmentAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AnthropicSelfHostedEnvironmentWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aws-external-anthropic:GetEnvironment",
        "aws-external-anthropic:GetSession",
        "aws-external-anthropic:GetSkill",
        "aws-external-anthropic:ProcessEnvironmentWork",
        "aws-external-anthropic:UpdateSession"
      ],
      "Resource" : "arn:aws:aws-external-anthropic:*:*:workspace/*"
    },
    {
      "Sid" : "AnthropicSelfHostedEnvironmentResourceless",
      "Effect" : "Allow",
```

```
      "Action" : [
        "aws-external-anthropic:CallWithBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

APIGatewayServiceRolePolicy

Descrição: permite que o API Gateway gerencie AWS os recursos associados em nome do cliente.

`APIGatewayServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 20 de outubro de 2017, 17:23 UTC
- Hora da edição: 12 de julho de 2021, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/amazon-apigateway-*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "acm:DescribeCertificate",
        "acm:GetCertificate"
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Owner",
            "VpcLinkId"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "servicediscovery:GetNamespace",
      "Resource" : "arn:aws:servicediscovery:*:*:namespace/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "servicediscovery:GetService",
      "Resource" : "arn:aws:servicediscovery:*:*:service/*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AppIntegrationsServiceLinkedRolePolicy

Descrição: Permite AppIntegrations gerenciar AppFlow recursos e publicar dados CloudWatch métricos em seu nome.

`AppIntegrationsServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 30 de setembro de 2022, 19:42 UTC
- Hora da edição: 30 de setembro de 2022, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AppIntegrations"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnectorEntity",
        "appflow:ListConnectorEntities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnectorProfiles",
        "appflow:UseConnectorProfile"
      ],
      "Resource" : "arn:aws:appflow:*:*:connector-profile/*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "appflow:DeleteFlow",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:StartFlow",
        "appflow:StopFlow",
        "appflow:UpdateFlow"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AppIntegrationsManaged" : "true"
        }
      },
      "Resource" : "arn:aws:appflow:*:*:flow/FlowCreatedByAppIntegrations-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:TagResource"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AppIntegrationsManaged"
          ]
        }
      },
      "Resource" : "arn:aws:appflow:*:*:flow/FlowCreatedByAppIntegrations-*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ApplicationAutoScalingForAmazonAppStreamAccess

Descrição: Política para habilitar o escalonamento automático de aplicativos para a Amazon AppStream

`ApplicationAutoScalingForAmazonAppStreamAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ApplicationAutoScalingForAmazonAppStreamAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 06 de fevereiro de 2017, 21:39 UTC
- Hora da edição: 06 de fevereiro de 2017, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

Descrição: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo recurso de exportação contínua do Application Discovery Service

`ApplicationDiscoveryServiceContinuousExportServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 09 de agosto de 2018, 20:22 UTC
- Hora da edição: 13 de agosto de 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:UpdateTable",
        "firehose:CreateDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "logs:CreateLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "firehose:DeleteDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:UpdateDestination"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
    },
    {
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::aws-application-discovery-service*"
    },
    {
      "Action" : [
        "s3:GetObject"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::aws-application-discovery-service*/*"
    },
    {
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutRetentionPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "firehose.amazonaws.com"
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "firehose.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AppRunnerNetworkingServiceRolePolicy

Descrição: Permite que o AWS AppRunner Networking gerencie AWS recursos relacionados em seu nome.

`AppRunnerNetworkingServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 12 de janeiro de 2022, 21:02 UTC
- Hora da edição: 12 de janeiro de 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AWSAppRunnerManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "StringLike" : {
          "aws:RequestTag/AWSAppRunnerManaged" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSAppRunnerManaged" : "false"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AppRunnerServiceRolePolicy

Descrição: Permite AWS AppRunner gerenciar AWS recursos relacionados em seu nome.

`AppRunnerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 14 de maio de 2021, 19:15 UTC
- Hora da edição: 14 de maio de 2021, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/apprunner/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/apprunner/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AWSAppRunnerManagedRule*"
    }
  ]
```

```
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AppStudioServiceRolePolicy

Descrição: Permite AppStudio gerenciar AWS recursos associados em seu nome.

`AppStudioServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 10 de julho de 2024, 5:01 UTC
- Horário editado: 13 de março de 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppStudioServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AppStudioResourcePermissionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appstudio/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AppStudioResourcePermissionsForSecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "IsAppStudioSecret"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/IsAppStudioSecret" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "AppStudioResourcePermissionsForManagedSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appstudio"
        }
      }
    },
    {
      "Sid" : "AppStudioResourceWritePermissionsForManagedSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AppStudioResourcePermissionsForSSO",
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso-directory:DescribeUsers",
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AssuranceServiceRolePolicy

Descrição: permite que o AWS Assurance acesse seus recursos para avaliações de conformidade e coleta de evidências.

`AssuranceServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 26 de agosto de 2026, 21:07 UTC
- Horário editado: 26 de agosto de 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AssuranceServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AssuranceComplianceRead",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAdjustmentTypes",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeAutoScalingNotificationTypes",
        "autoscaling:DescribeInstanceRefreshes",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHookTypes",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribeLoadBalancerTargetGroups",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeMetricCollectionTypes",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScalingProcessTypes",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeTerminationPolicyTypes",
        "autoscaling:DescribeTrafficSources",
        "autoscaling:DescribeWarmPool",
        "bedrock-agentcore:GetAgentCard",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetResourcePolicy",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:GetWorkloadIdentity",
```

```
        "bedrock-agentcore:ListActors",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimeVersions",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBrowserProfiles",
        "bedrock-agentcore:ListBrowserSessions",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListCodeInterpreterSessions",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListEvents",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListMemoryExtractionJobs",
        "bedrock-agentcore:ListMemoryRecords",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListSessions",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentMemory",
        "bedrock:GetAgentVersion",
        "bedrock:GetCustomModel",
        "bedrock:GetDataSource",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowExecution",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetGuardrail",
        "bedrock:GetIngestionJob",
        "bedrock:GetInvocationStep",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPrompt",
```

```
        "bedrock:GetSession",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgentVersions",
        "bedrock:ListAgents",
        "bedrock:ListAutomatedReasoningPolicies",
        "bedrock:ListBlueprints",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlowExecutionEvents",
        "bedrock:ListFlowExecutions",
        "bedrock:ListFlowVersions",
        "bedrock:ListFlows",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListIngestionJobs",
        "bedrock:ListInvocationSteps",
        "bedrock:ListInvocations",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPrompts",
        "bedrock:ListSessions",
        "bedrock:ListTagsForResource",
        "bedrock:ValidateFlowDefinition",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListStackResources",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetQueryResults",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListChannels",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartQuery",
        "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:GetMetricData",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetrics",
        "config:DescribeComplianceByConfigRule",
        "config:DescribeConfigRules",
        "config:DescribeConfigurationAggregators",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConformancePacks",
        "config:DescribeOrganizationConformancePacks",
        "config:GetComplianceDetailsByConfigRule",
        "config:SelectResourceConfig",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListBackups",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumeAttribute",
```

```
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEncryptionControls",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeImages",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeDaemon",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:DescribeTasks",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListDaemons",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeAddonVersions",
        "eks:DescribeCapability",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
```

```
        "eks:DescribePodIdentityAssociation",
        "eks:DescribeUpdate",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListCapabilities",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "eks:ListTagsForResource",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:ListTagsForResource",
        "events:ListTagsForResource",
        "events:DescribeEventBus",
        "guardduty:DescribeOrganizationConfiguration",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFindings",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatEntitySets",
        "guardduty:ListThreatIntelSets",
        "guardduty:ListTrustedEntitySets",
        "iam:GenerateCredentialReport",
        "iam:GetAccessKeyLastUsed",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
```

```
        "iam:GetGroupPolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListMFADevices",
        "iam:ListPolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lambda:GetFunction",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListCapacityProviders",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListFunctions",
        "lambda:ListLayerVersions",
        "lambda:ListLayers",
        "lambda:ListTags",
```

```
        "lambda:ListVersionsByFunction",
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeResourcePolicies",
        "logs:DescribeSubscriptionFilters",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "logs:GetQueryResults",
        "logs:StartQuery",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventSubscriptions",
        "rds:ListTagsForResource",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
```

```
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "securityhub:BatchGetSecurityControls",
        "securityhub:DescribeHub",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindings",
        "securityhub:ListSecurityControlDefinitions",
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ApiGatewayRead",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "OrganizationsTopologyRead",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListParents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AssuranceConfigurationRecorderManagement",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders",
        "config:PutServiceLinkedConfigurationRecorder"
      ],
      "Resource" : "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForAssurance/*"
    },
    {
      "Sid" : "AWSConfigServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AssurancePolicy",
      "Effect" : "Allow",
      "Action" : [
        "assurance:CreateComment",
        "assurance:DownloadEvidence",
        "assurance:GetAssessment",
        "assurance:GetComment",
```

```
        "assurance:GetControl",
        "assurance:GetEnvironment",
        "assurance:GetEvidence",
        "assurance:GetProject",
        "assurance:GetTask",
        "assurance:ListAssessmentAnnotations",
        "assurance:ListAssessments",
        "assurance:ListComments",
        "assurance:ListControls",
        "assurance:ListDiscoveredResources",
        "assurance:ListEnabledFrameworks",
        "assurance:ListEvidence",
        "assurance:ListEvidenceAnnotations",
        "assurance:ListProjects",
        "assurance:ListTasks",
        "assurance:StartResourceDiscovery",
        "assurance:UpdateTask",
        "assurance:UploadEvidence"
      ],
      "Resource" : "arn:*:assurance:*:*:environment/*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AuroraDsqlServiceLinkedRolePolicy

Descrição: política para a função vinculada ao serviço do Amazon Aurora DSQL.

`AuroraDsqlServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 03 de dezembro de 2024, 15:06 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AuroraDsqlServiceLinkedRolePolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/AuroraDSQL",
            "AWS/Usage"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AutoScalingConsoleFullAccess

Descrição: Fornece acesso total ao Auto Scaling por meio do Console de gerenciamento da AWS.

`AutoScalingConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AutoScalingConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 12 de janeiro de 2017, 19:43 UTC
- Hora da edição: 06 de fevereiro de 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateKeyPair",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:ImportKeyPair"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListSubscriptions",
```

```
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AutoScalingConsoleReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Auto Scaling por meio do. Console de gerenciamento da AWS

`AutoScalingConsoleReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AutoScalingConsoleReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 12 de janeiro de 2017, 19:48 UTC
- Hora da edição: 12 de janeiro de 2017, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
```

```
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListSubscriptions",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AutoScalingFullAccess

Descrição: fornece acesso total ao Auto Scaling.

`AutoScalingFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AutoScalingFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 12 de janeiro de 2017, 19:31 UTC
- Hora da edição: 06 de fevereiro de 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricAlarm",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcClassicLink"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AutoScalingNotificationAccessRole

Descrição: Política padrão para a função de serviço AutoScaling Notification Access.

`AutoScalingNotificationAccessRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AutoScalingNotificationAccessRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AutoScalingReadOnlyAccess

Descrição: fornece acesso somente leitura ao Auto Scaling.

`AutoScalingReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AutoScalingReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 12 de janeiro de 2017, 19:39 UTC
- Hora da edição: 12 de janeiro de 2017, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AutoScalingServiceRolePolicy

Descrição: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo Auto Scaling

`AutoScalingServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 08 de janeiro de 2018, 23:10 UTC
- Horário editado: 12 de novembro de 2025, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachClassicLinkVpc",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateReplaceRootVolumeTask",
        "ec2:CreateFleet",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:DetachClassicLinkVpc",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2InstanceProfileManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "EC2SpotManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ELBManagement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Register*",
        "elasticloadbalancing:Deregister*",
        "elasticloadbalancing:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWManagement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSManagement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridgeRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemsManagerParameterManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcLatticeManagement",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeregisterTargets",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListTargets",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:RegisterTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsManagement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWS-SSM-Automation-DiagnosisBucketPolicy

Descrição: concede permissões para acessar o bucket do S3 de diagnóstico do SSM para fins de diagnóstico e correção de problemas.

`AWS-SSM-Automation-DiagnosisBucketPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWS-SSM-Automation-DiagnosisBucketPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 15 de novembro de 2024, 23:31 UTC
- Horário editado: 15 de novembro de 2024, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-Automation-DiagnosisBucketPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*/
${aws:PrincipalAccount}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*/
${aws:PrincipalAccount}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    },
    {
      "Sid" : "AllowReadOnlyAccessListBucketOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
```

```
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : "*/${aws:PrincipalAccount}/*"
        }
      }
    },
    {
      "Sid" : "AllowReadOnlyAccessListBucketOnSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        },
        "StringLike" : {
          "s3:prefix" : "*/${aws:PrincipalAccount}/*"
        }
      }
    },
    {
      "Sid" : "AllowGetEncryptionConfigurationOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowGetEncryptionConfigurationOnSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
```

```
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy

Descrição: fornece permissão para diagnosticar problemas com os serviços SSM, executando as atividades definidas nos documentos de automação. Usada principalmente para executar os documentos de automação em uma configuração entre contras e entre regiões ao acionar automações secundárias nas contas de membros.

`AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 16 de novembro de 2024, 00:01 UTC
- Horário editado: 29 de agosto de 2026, 00:47 UTC

- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-*UnmanagedEC2*",
        "arn:aws:ssm:*:*:document/AWS-DiagnoseHybridActivationIssues",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-*UnmanagedEC2*:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-DiagnoseHybridActivationIssues:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAssumeDiagnosisExecutionRoleWithinAccount",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisAdminRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListBucketOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy

Descrição: Forneça permissão para diagnosticar problemas com serviços SSM executando atividades definidas nos Documentos de Automação, usados principalmente para executar os documentos de Automação em uma account/region configuração de destino, diagnosticando a integridade do serviço SSM em todos os nós.

`AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 16 de novembro de 2024, 00:08 UTC
- Horário editado: 28 de agosto de 2026, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessEC2Resource",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeNetworkAcls"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetConsoleOutput",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationStepExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeActivations",
        "ssm:GetAutomationExecution",
        "ssm:GetServiceSetting"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyAccessIAMResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRole",
```

```
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-*UnmanagedEC2*",
        "arn:aws:ssm:*:*:document/AWS-DiagnoseHybridActivationIssues",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-*UnmanagedEC2*:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-DiagnoseHybridActivationIssues:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
```

```
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy

Descrição: fornece permissões para contas operacionais diagnosticarem nós não gerenciados, fornecendo permissões específicas da organização exigidas pela automação do SSM para extrair a lista de contas membros de uma raiz de uma organização para acionar a execução entre contas entre regiões, permitindo assumir funções de execução no destino. account/region

`AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Horário de criação: 16 de novembro de 2024, 00:11 UTC
- Horário editado: 16 de novembro de 2024, 00:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessOrganization",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeDiagnosisExecutionRoleWithinOrg",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWS-SSM-RemediationAutomation-AdministrationRolePolicy

Descrição: fornece permissão para corrigir problemas com os serviços SSM, executando as atividades definidas nos documentos de automação. Usada principalmente para executar os documentos de automação em uma configuração entre contras e entre regiões ao acionar automações secundárias nas contas de membros.

`AWS-SSM-RemediationAutomation-AdministrationRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWS-SSM-RemediationAutomation-AdministrationRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 16 de novembro de 2024, 00:14 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-AdministrationRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-OrchestrateUnmanagedEC2Actions",
        "arn:aws:ssm:*:*:document/AWS-RemediateSSMAgent*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-OrchestrateUnmanagedEC2Actions:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RemediateSSMAgent*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
```

```
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAssumeRemediationExecutionRoleWithinAccount",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationAdminRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListBucketOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWS-SSM-RemediationAutomation-ExecutionRolePolicy

Descrição: fornece permissões para corrigir problemas com serviços de SSM executando atividades definidas nos Documentos de Automação, usados principalmente para executar os documentos de automação em uma account/region configuração de destino, corrigindo a integridade dos serviços de SSM em todos os nós.

`AWS-SSM-RemediationAutomation-ExecutionRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWS-SSM-RemediationAutomation-ExecutionRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 16 de novembro de 2024, 00:17 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-ExecutionRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyAccessEC2Resource",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateVpcEndpointForTaggedSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
        }
      }
    },
    {
      "Sid" : "AllowCreateVpcEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "RestrictCreateVpcEndpointForSSMService",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
```

```
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.ssm",
            "com.amazonaws.*.ssmmessages",
            "com.amazonaws.*.ec2messages"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingVPCEndpoints::VPCE" :
"VPCEndpoint"
        }
      }
    },
    {
      "Sid" : "RestrictCreateVpcEndpointWithTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingVPCEndpoints::VPCE" :
"VPCEndpoint",
          "ec2:CreateAction" : [
            "CreateVpcEndpoint"
          ]
        }
      }
    },
    {
      "Sid" : "AllowModifyVpcAttributeForDns",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Attribute" : [
            "EnableDnsSupport",
```

```
            "EnableDnsHostnames"
          ]
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdateForTaggedResource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdateWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::SG::Rule" :
"HTTPSAccess"
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdateTagRule",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::SG::Rule" :
"HTTPSAccess",
          "ec2:CreateAction" : [
            "AuthorizeSecurityGroupEgress",
            "AuthorizeSecurityGroupIngress"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCreateSecurityGroupForVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "AllowCreateSecurityGroupWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
        }
      }
    },
    {
      "Sid" : "AllowTagCreationForSecurityGroupTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup",
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-OrchestrateUnmanagedEC2Actions",
        "arn:aws:ssm:*:*:document/AWS-RemediateSSMAgent*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-OrchestrateUnmanagedEC2Actions:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RemediateSSMAgent*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy

Descrição: fornece permissões para contas operacionais corrigirem nós não gerenciados, fornecendo permissões específicas à organização exigidas pela automação do SSM para extrair a lista de contas membros de uma raiz de uma organização para acionar a execução entre contas entre regiões, permitindo assumir funções de execução no destino. account/region

`AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 16 de novembro de 2024, 00:25 UTC
- Horário editado: 16 de novembro de 2024, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "AllowReadOnlyAccessOrganization",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeRemediationExecutionRoleWithinOrg",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWS_ ConfigRole

Descrição: Política padrão para a função de serviço AWS Config. Fornece as permissões necessárias para que o AWS Config acompanhe as alterações em seus AWS recursos.

`AWS_ConfigRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWS_ConfigRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 15 de setembro de 2020, 20:30 UTC
- Horário editado: 23 de setembro de 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWS_ConfigRole`

Versão da política

Versão da política: v73 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigRoleStatementID1",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "access-analyzer:ValidatePolicy",
        "account-access:GetEntitlement",
        "account-access:ListEntitlements",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
```

```
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListTagsForResource",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListForms",
        "amplifyuibuilder:ListThemes",
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "apigateway:GET",
        "app-integrations:GetApplication",
        "app-integrations:GetDataIntegration",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListApplications",
        "app-integrations:ListDataIntegrations",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
        "app-integrations:ListTagsForResource",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
```

```
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExperimentDefinition",
        "appconfig:GetExtension",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExperimentDefinitions",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource",
        "applicationinsights:DescribeApplication",
        "applicationinsights:DescribeComponent",
        "applicationinsights:DescribeLogPattern",
        "applicationinsights:ListApplications",
        "applicationinsights:ListComponents",
        "applicationinsights:ListLogPatterns",
        "applicationinsights:ListLogPatternSets",
        "applicationinsights:ListTagsForResource",
        "appmesh:DescribeGatewayRoute",
        "appmesh:DescribeMesh",
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
```

```
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:DescribeAppBlockBuilders",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appstream:ListAssociatedFleets",
        "appstream:ListAssociatedStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApi",
        "appsync:GetApiAssociation",
        "appsync:GetApiCache",
        "appsync:GetChannelNamespace",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetGraphqlApi",
        "appsync:GetResolver",
        "appsync:GetSourceApiAssociation",
        "appsync:ListApis",
        "appsync:ListChannelNamespaces",
        "appsync:ListDataSources",
        "appsync:ListDomainNames",
        "appsync:ListGraphqlApis",
        "appsync:ListResolvers",
        "appsync:ListSourceApiAssociations",
```

```
        "appsync:ListTagsForResource",
        "appsync:ListTypes",
        "apptest:GetTestCase",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeAnomalyDetector",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration",
        "aps:DescribeResourcePolicy",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeScraperLoggingConfiguration",
        "aps:DescribeWorkspace",
        "aps:DescribeWorkspaceConfiguration",
        "aps:ListAnomalyDetectors",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "arc-region-switch:GetPlan",
        "arc-region-switch:ListPlans",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListTagsForResource",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetControl",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessments",
        "auditmanager:ListControls",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
```

```
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "b2bi:GetCapability",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:GetTransformer",
        "b2bi:ListCapabilities",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "b2bi:ListTagsForResource",
        "b2bi:ListTransformers",
        "backup-gateway:GetHypervisor",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:GetTieringConfiguration",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListRestoreTestingPlans",
        "backup:ListRestoreTestingSelections",
        "backup:ListTags",
        "backup:ListTieringConfigurations",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeConsumableResource",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobQueues",
```

```
        "batch:DescribeQuotaShare",
        "batch:DescribeSchedulingPolicies",
        "batch:DescribeServiceEnvironments",
        "batch:ListConsumableResources",
        "batch:ListQuotaShares",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "bcm-dashboards:GetDashboard",
        "bcm-dashboards:ListDashboards",
        "bcm-dashboards:ListTagsForResource",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:ListExports",
        "bcm-data-exports:ListTagsForResource",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetBrowserProfile",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetConfigurationBundle",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPaymentConnector",
        "bedrock-agentcore:GetPaymentCredentialProvider",
        "bedrock-agentcore:GetPaymentManager",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetPolicyEngineSummary",
        "bedrock-agentcore:GetPolicyGeneration",
        "bedrock-agentcore:GetPolicyGenerationSummary",
        "bedrock-agentcore:GetPolicySummary",
        "bedrock-agentcore:GetResourcePolicy",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBrowserProfiles",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListCodeInterpreters",
```

```
        "bedrock-agentcore:ListConfigurationBundles",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:ListPaymentConnectors",
        "bedrock-agentcore:ListPaymentCredentialProviders",
        "bedrock-agentcore:ListPaymentManagers",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListPolicyEngineSummaries",
        "bedrock-agentcore:ListPolicyGenerations",
        "bedrock-agentcore:ListPolicyGenerationSummaries",
        "bedrock-agentcore:ListPolicySummaries",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAutomatedReasoningPolicy",
        "bedrock:GetBlueprint",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataSource",
        "bedrock:GetEvaluationJob",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPromptRouter",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAutomatedReasoningPolicies",
        "bedrock:ListBlueprints",
```

```
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListDataSources",
        "bedrock:ListEnforcedGuardrailsConfiguration",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListFlowVersions",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "billing:GetBillingView",
        "billing:ListBillingViews",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "braket:ListTagsForResource",
        "braket:SearchSpendingLimits",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cases:BatchGetCaseRule",
        "cases:BatchGetField",
        "cases:GetDomain",
        "cases:GetLayout",
        "cases:GetTemplate",
        "cases:ListCaseRules",
        "cases:ListDomains",
        "cases:ListFields",
        "cases:ListLayouts",
        "cases:ListTemplates",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetAnomalyMonitors",
```

```
        "ce:GetAnomalySubscriptions",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "chime:DescribeAppInstance",
        "chime:DescribeAppInstanceBot",
        "chime:DescribeAppInstanceUser",
        "chime:DescribeChannelFlow",
        "chime:ListAppInstanceBots",
        "chime:ListAppInstances",
        "chime:ListChannelFlows",
        "chime:ListTagsForResource",
        "cleanrooms-ml:GetConfiguredModelAlgorithm",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListConfiguredModelAlgorithms",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListTagsForResource",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribePublisher",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
```

```
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListChangeSets",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
        "cloudfront:DescribeFunction",
        "cloudfront:DescribeKeyValueStore",
        "cloudfront:GetAnycastIpList",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetConnectionGroup",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistributionTenant",
        "cloudfront:GetFunction",
        "cloudfront:GetKeyGroup",
        "cloudfront:GetMonitoringSubscription",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:GetVpcOrigin",
        "cloudfront:ListAnycastIpLists",
        "cloudfront:ListCachePolicies",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListConnectionGroups",
        "cloudfront:ListContinuousDeploymentPolicies",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListFunctions",
        "cloudfront:ListKeyGroups",
        "cloudfront:ListKeyValueStores",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudfront:ListVpcOrigins",
```

```
        "cloudtrail:DescribeTrails",
        "cloudTrail:GetChannel",
        "cloudtrail:GetDashboard",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudTrail:ListChannels",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:DescribeInsightRules",
        "cloudwatch:GetAlarmMuteRule",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListAlarmMuteRules",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListManagedInsightRules",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackageGroup",
        "codeartifact:DescribeRepository",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListAllowedRepositoriesForGroup",
        "codeartifact:ListDomains",
        "codeartifact:ListPackageGroups",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetFleets",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListFleets",
        "codebuild:ListReportGroups",
        "codebuild:ListSourceCredentials",
```

```
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codedeploy:GetDeploymentConfig",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "codepipeline:ListWebhooks",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:ListConnections",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListTagsForResource",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:AdminGetUser",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeManagedLoginBranding",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeTerms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
```

```
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListTerms",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "comprehend:DescribeFlywheel",
        "comprehend:ListFlywheels",
        "comprehend:ListTagsForResource",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:ListCampaigns",
        "connect:DescribeAgentStatus",
        "connect:DescribeDataTable",
        "connect:DescribeEmailAddress",
        "connect:DescribeEvaluationForm",
        "connect:DescribeHoursOfOperation",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribeMetric",
        "connect:DescribeNotification",
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUser",
        "connect:DescribeUserHierarchyGroup",
        "connect:DescribeUserHierarchyStructure",
        "connect:DescribeView",
        "connect:DescribeWorkspace",
        "connect:GetTaskTemplate",
        "connect:ListAgentStatuses",
        "connect:ListApprovedOrigins",
        "connect:ListDataTables",
```

```
        "connect:ListEvaluationForms",
        "connect:ListEvaluationFormVersions",
        "connect:ListHoursOfOperationOverrides",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListMetrics",
        "connect:ListNotifications",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPredefinedAttributes",
        "connect:ListPrompts",
        "connect:ListQueueEmailAddresses",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileManualAssignmentQueues",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileAIAgents",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfileFlowModules",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListTrafficDistributionGroups",
        "connect:ListUserHierarchyGroups",
        "connect:ListUsers",
        "connect:ListViews",
        "connect:ListViewVersions",
        "connect:ListWorkspaceMedia",
        "connect:ListWorkspacePages",
        "connect:ListWorkspaces",
        "connect:SearchAvailablePhoneNumbers",
        "connect:SearchWorkspaceAssociations",
        "controltower:GetLandingZone",
        "controltower:ListLandingZones",
        "cur:DescribeReportDefinitions",
        "cur:ListTagsForResource",
```

```
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationAzureBlob",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxOntap",
        "datasync:DescribeLocationFsxOpenZfs",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentProfile",
        "datazone:GetGroupProfile",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListDomains",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurations",
```

```
        "datazone:ListEnvironmentProfiles",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListSubscriptionTargets",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "deadline:GetBudget",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetJob",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetQueueLimitAssociation",
        "deadline:GetStorageProfile",
        "deadline:ListBudgets",
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListJobs",
        "deadline:ListLicenseEndpoints",
        "deadline:ListMonitors",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListQueueLimitAssociations",
        "deadline:ListQueues",
        "deadline:ListStorageProfiles",
        "deadline:ListTagsForResource",
        "deadline:SearchJobs",
        "detective:ListGraphs",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
```

```
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListNotificationChannels",
        "directconnect:DescribeConnections",
        "dms:DescribeCertificates",
        "dms:DescribeDataMigrations",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationConfigs",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListDataProviders",
        "dms:ListInstanceProfiles",
        "dms:ListMigrationProjects",
        "dms:ListTagsForResource",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dsql:GetCluster",
        "dsql:GetClusterPolicy",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
```

```
        "ec2:Describe*",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeTransitGatewayMeteringPolicies",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetRouteServerAssociations",
        "ec2:GetRouteServerPropagations",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:DescribeRepositoryCreationTemplates",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeExpressGatewayService",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
```

```
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeCapability",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListCapabilities",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:DescribeCapacityReservation",
        "elasticloadbalancing:DescribeListenerAttributes",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
```

```
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "elemental-inference:GetFeed",
        "elemental-inference:ListFeeds",
        "elemental-inference:ListTagsForResource",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetIdNamespace",
        "entityresolution:GetMatchingWorkflow",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
```

```
        "entityresolution:ListIdNamespaces",
        "entityresolution:ListMatchingWorkflows",
        "entityresolution:ListSchemaMappings",
        "entityresolution:ListTagsForResource",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:ListExperimentTemplates",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fms:GetNotificationChannel",
```

```
        "fms:GetPolicy",
        "fms:ListPolicies",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "forecast:ListTagsForResource",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeFileSystems",
        "fsx:DescribeS3AccessPointAttachments",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeContainerFleet",
        "gamelift:DescribeContainerGroupDefinition",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScalingPolicies",
```

```
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListContainerFleets",
        "gamelift:ListContainerGroupDefinitions",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "gamelift:ValidateMatchmakingRuleSet",
        "gameliftstreams:GetApplication",
        "gameliftstreams:GetStreamGroup",
        "gameliftstreams:ListApplications",
        "gameliftstreams:ListStreamGroups",
        "gameliftstreams:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeKey",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListKeys",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeAcceleratorAttributes",
        "globalaccelerator:DescribeCrossAccountAttachment",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCrossAccountAttachments",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
```

```
        "glue:DescribeIntegrations",
        "glue:GetBlueprint",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetRegistry",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetSession",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetWorkflow",
        "glue:ListBlueprints",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListSessions",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:GetDeployment",
        "greengrass:ListComponents",
```

```
        "greengrass:ListComponentVersions",
        "greengrass:ListDeployments",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatEntitySet",
        "guardduty:GetThreatIntelSet",
        "guardduty:GetTrustedEntitySet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatEntitySets",
        "guardduty:ListThreatIntelSets",
        "guardduty:ListTrustedEntitySets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:GetDataTransformationProfile",
        "healthlake:ListDataTransformationProfiles",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
```

```
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
        "iam:ListMFADeviceTags",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
```

```
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
        "imagebuilder:ListWorkflowBuildVersions",
        "imagebuilder:ListWorkflows",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetCodeSecurityScanConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListCodeSecurityScanConfigurations",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "inspector2:ListTagsForResource",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:ListTagsForResource",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCertificateProvider",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJob",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
```

```
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetCommand",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:GetV2LoggingOptions",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificateProviders",
        "iot:ListCertificates",
        "iot:ListCommands",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPackages",
        "iot:ListPackageVersions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
```

```
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetStateTemplate",
        "iotfleetwise:GetVehicle"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigRoleStatementID2",
      "Effect" : "Allow",
      "Action" : [
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListStateTemplates",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeAccessPolicy",
```

```
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeComputationModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeDataset",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListComputationModels",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
```

```
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListDevicesForWirelessDeviceImportTask",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStorageConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
```

```
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListTagsForResource",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra-ranking:DescribeRescoreExecutionPlan",
        "kendra-ranking:ListRescoreExecutionPlans",
        "kendra-ranking:ListTagsForResource",
        "kendra:DescribeIndex",
        "kendra:ListDataSources",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetResourcePolicy",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeLakeFormationIdentityCenterConfiguration",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
```

```
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionScalingConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListCapacityProviders",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctions",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "launchwizard:GetDeployment",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListTagsForResource",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
```

```
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "license-manager:ListTagsForResource",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperations",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeDestinations",
        "logs:DescribeIndexPolicies",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
```

```
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetIntegration",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindingsFilters",
        "macie2:ListTagsForResource",
        "managedblockchain:GetAccessor",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListAccessors",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
```

```
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeGateway",
        "mediaconnect:GetRouterInput",
        "mediaconnect:GetRouterNetworkInterface",
        "mediaconnect:ListBridges",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGateways",
        "mediaconnect:ListRouterInputs",
        "mediaconnect:ListRouterNetworkInterfaces",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListTagsForResource",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeNode",
        "medialive:DescribeSdiSource",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:ListChannelPlacementGroups",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListMultiplexes",
        "medialive:ListMultiplexPrograms",
        "medialive:ListNodes",
        "medialive:ListSdiSources",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:DescribeAsset",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
```

```
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediatailor:DescribeChannel",
        "mediatailor:DescribeLiveSource",
        "mediatailor:DescribeSourceLocation",
        "mediatailor:DescribeVodSource",
        "mediatailor:GetChannelPolicy",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "medical-imaging:GetDatastore",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListTagsForResource",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetEmailChannel",
        "mobiletargeting:GetEmailTemplate",
        "mobiletargeting:GetEventStream",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:GetSegment",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTagsForResource",
        "mobiletargeting:ListTemplates",
        "mpa:GetIdentitySource",
        "mpa:ListIdentitySources",
        "mpa:ListTagsForResource",
        "mq:DescribeBroker",
        "mq:DescribeConfiguration",
```

```
        "mq:ListBrokers",
        "mq:ListConfigurations",
        "mq:ListTags",
        "neptune-graph:GetGraphSnapshot",
        "neptune-graph:ListGraphSnapshots",
        "neptune-graph:ListTagsForResource",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetDirectConnectGatewayAttachment",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:ListTagsForResource",
        "notifications:GetEventRule",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
```

```
        "notifications:ListOrganizationalUnits",
        "notifications:ListTagsForResource",
        "nova-act:GetWorkflowDefinition",
        "nova-act:ListWorkflowDefinitions",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListLinks",
        "oam:ListSinks",
        "oam:ListTagsForResource",
        "omics:GetAnnotationStore",
        "omics:GetConfiguration",
        "omics:GetReferenceStore",
        "omics:GetRun",
        "omics:GetRunCache",
        "omics:GetRunGroup",
        "omics:GetS3AccessPolicy",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:GetWorkflowVersion",
        "omics:ListAnnotationStores",
        "omics:ListConfigurations",
        "omics:ListReferenceStores",
        "omics:ListRunCaches",
        "omics:ListRunGroups",
        "omics:ListRuns",
        "omics:ListSequenceStores",
        "omics:ListTagsForResource",
        "omics:ListVariantStores",
        "omics:ListWorkflows",
        "omics:ListWorkflowVersions",
        "opsworks:DescribeInstances",
        "opsworks:DescribeLayers",
        "opsworks:DescribeTimeBasedAutoScaling",
        "opsworks:DescribeVolumes",
        "opsworks:ListTags",
        "organizations:DescribeAccount",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
```

```
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "osis:GetPipeline",
        "osis:GetResourcePolicy",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "outposts:GetSite",
        "outposts:ListSites",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListChallengeMetadata",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
```

```
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetPolicy",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:ListApplications",
        "qbusiness:ListDataSources",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeCustomPermissions",
```

```
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeOAuthClientApplication",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:DescribeTopic",
        "quicksight:DescribeVPCConnection",
        "quicksight:ListAnalyses",
        "quicksight:ListCustomPermissions",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListFolders",
        "quicksight:ListOAuthClientApplications",
        "quicksight:ListRefreshSchedules",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "quicksight:ListTopics",
        "quicksight:ListVPCConnections",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
```

```
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterDbRevisions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeDataShares",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
```

```
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:DescribeCollection",
        "rekognition:DescribeProjects",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListCollections",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "robomaker:DescribeRobotApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListRobotApplications",
        "robomaker:ListSimulationApplications",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-control-config:DescribeCluster",
```

```
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
```

```
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListOutpostResolvers",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver:ListTagsForResource",
        "rtbfabric:GetCertificateAssociation",
        "rtbfabric:GetInboundExternalLink",
        "rtbfabric:GetLink",
        "rtbfabric:GetLinkRoutingRule",
        "rtbfabric:GetOutboundExternalLink",
        "rtbfabric:GetRequesterGateway",
        "rtbfabric:GetResponderGateway",
        "rtbfabric:ListCertificateAssociations",
        "rtbfabric:ListLinkRoutingRules",
        "rtbfabric:ListLinks",
        "rtbfabric:ListRequesterGateways",
        "rtbfabric:ListResponderGateways",
        "rtbfabric:ListTagsForResource",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
```

```
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
```

```
        "s3:ListTagsForResource",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:GetMetricsConfiguration",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListTagsForResource",
        "s3files:GetAccessPoint",
        "s3files:GetFileSystem",
        "s3files:GetFileSystemPolicy",
        "s3files:GetMountTarget",
        "s3files:GetSynchronizationConfiguration",
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems",
        "s3files:ListMountTargets",
        "s3files:ListTagsForResource",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketMetricsConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:ListTableBuckets",
        "s3tables:ListTagsForResource",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:ListIndexes",
        "s3vectors:ListTagsForResource",
        "s3vectors:ListVectorBuckets",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeClusterSchedulerConfig",
```

```
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeComputeQuota",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHub",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeMlflowApp",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelCardExportJob",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribePartnerApp",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTrainingPlan",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
```

```
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListClusters",
        "sagemaker:ListClusterSchedulerConfigs",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListComputeQuotas",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHubs",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListMlflowApps",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCardExportJobs",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringSchedules",
```

```
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListOptimizationJobs",
        "sagemaker:ListPartnerApps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSpaces",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingPlans",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "sdb:GetAttributes",
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetTargetDomains",
        "securityagent:GetApplication",
        "securityagent:ListApplications",
        "securityagent:ListPentests",
        "securityagent:ListTagsForResource",
        "securityagent:ListTargetDomains",
        "securityhub:DescribeHub",
```

```
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetAggregatorV2",
        "securityhub:GetAutomationRuleV2",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:ListAggregatorsV2",
        "securityhub:ListAutomationRulesV2",
        "securityhub:ListConfigurationPolicies",
        "securityhub:ListConfigurationPolicyAssociations",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:ListFindingAggregators",
        "securityhub:ListTagsForResource",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "serviceCatalog:DescribePortfolioShares",
        "servicecatalog:DescribeServiceAction",
        "servicecatalog:DescribeTagOption",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListServiceActions",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:ListTagOptions",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetAddonInstance",
        "ses:GetAddonSubscription",
        "ses:GetAddressList",
```

```
        "ses:GetArchive",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailTemplate",
        "ses:GetIngressPoint",
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:ListAddonInstances",
        "ses:ListAddonSubscriptions",
        "ses:ListAddressLists",
        "ses:ListArchives",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailTemplates",
        "ses:ListIngressPoints",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListRelays",
        "ses:ListRuleSets",
        "ses:ListTagsForResource",
        "ses:ListTemplates",
        "ses:ListTrafficPolicies",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeProtectionGroup",
        "shield:DescribeSubscription",
        "shield:ListProtectionGroups",
        "shield:ListTagsForResource",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeProtectConfigurations",
        "sms-voice:DescribeSenderIds",
```

```
        "sms-voice:GetProtectConfigurationCountryRuleSet",
        "sms-voice:GetResourcePolicy",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:GetRotation",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListRotations",
        "ssm-contacts:ListTagsForResource",
        "ssm-guiconnect:GetConnectionRecordingPreferences",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:ListTagsForResource",
        "ssm:DescribeAssociation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm:GetAutomationExecution",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetMaintenanceWindow",
        "ssm:GetPatchBaseline",
```

```
        "ssm:GetResourcePolicies",
        "ssm:GetServiceSetting",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso:DescribeApplication",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:ListApplications",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineAlias",
        "states:ListActivities",
        "states:ListStateMachineAliases",
        "states:ListStateMachines",
        "states:ListStateMachineVersions",
        "states:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "textract:GetAdapter",
        "textract:ListAdapters",
        "textract:ListTagsForResource",
        "timestream-influxdb:GetDbCluster",
```

```
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transcribe:GetCallAnalyticsJob",
        "transcribe:GetVocabularyFilter",
        "transcribe:ListCallAnalyticsJobs",
        "transcribe:ListTagsForResource",
        "transcribe:ListVocabularyFilters",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWebApp",
        "transfer:DescribeWebAppCustomization",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWebApps",
        "transfer:ListWorkflows",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "verifiedpermissions:ListTagsForResource",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
```

```
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wisdom:GetAIAgent",
        "wisdom:GetAIGuardrail",
        "wisdom:GetAIPrompt",
        "wisdom:GetAssistant",
        "wisdom:ListAIAgentVersions",
        "wisdom:ListAIGuardrails",
        "wisdom:ListAIGuardrailVersions",
        "wisdom:ListAIPromptVersions",
        "wisdom:ListAssistants",
        "workspaces-web:GetNetworkSettings",
```

```
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIpAccessSettings",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetIndexingRules",
        "xray:GetSamplingRules",
        "xray:GetTraceSegmentDestination",
        "xray:ListResourcePolicies",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConfigLogStreamStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "ConfigLogEventsStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAccountActivityAccess

Descrição: permite que os usuários acessem a página de atividades da conta.

`AWSAccountActivityAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAccountActivityAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 20 de fevereiro de 2026, 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountActivityAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "payments:ListPaymentPreferences"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAccountManagementFullAccess

Descrição: Fornece acesso total ao gerenciamento de AWS contas.

`AWSAccountManagementFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAccountManagementFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de setembro de 2021, 23:20 UTC
- Hora da edição: 30 de setembro de 2021, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "account:*",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAccountManagementReadOnlyAccess

Descrição: Fornece acesso somente para AWS leitura ao gerenciamento de contas

`AWSAccountManagementReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAccountManagementReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de setembro de 2021, 23:29 UTC
- Hora da edição: 30 de setembro de 2021, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:Get*",
        "account:List*"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAccountSettingsManagementRole

Descrição: fornece as permissões necessárias para gerenciar uma conta para AWS aplicativos.

`AWSAccountSettingsManagementRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAccountSettingsManagementRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 11 de dezembro de 2025, 17:49 UTC
- Horário editado: 30 de setembro de 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountSettingsManagementRole`

Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetContactInformation",
        "account:PutContactInformation",
        "account:GetAccountInformation",
        "account:CloseAccount",
        "account:SendPhoneNumberVerification",
        "account:VerifyPhoneNumber"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "payments:ListTagsForResource",
        "payments:UntagResource",
        "payments:TagResource",
        "payments:ListPaymentPreferences",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:MakePayment",
        "payments:UpdatePaymentPreferences",
        "payments:CreatePaymentInstrument",
        "payments:UpdatePaymentInstrument",
        "payments:DeletePaymentInstrument",
        "payments:ListPaymentInstruments"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "invoicing:GetInvoicePDF"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "billing:GetSellerOfRecord"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ce:GetCostAndUsage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tax:GetTaxRegistration",
        "tax:PutTaxRegistration",
        "tax:ListTaxRegistrations",
        "tax:DeleteTaxRegistration",
        "tax:BatchPutTaxRegistration",
        "tax:GetTaxRegistrationDocument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
```

```
        "customer-verification:CreateCustomerVerificationDetails",
        "customer-verification:CreateUploadUrls",
        "customer-verification:UpdateCustomerVerificationDetails"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:ListApplications",
        "sso:DescribeApplication",
        "sso:DescribeInstance"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeCases",
        "support:AddCommunicationToCase",
        "support:ResolveCase",
        "support:AddAttachmentsToSet",
        "support:DescribeAttachment",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAccountUsageReportAccess

Descrição: permite que os usuários acessem a página de relatório de uso da conta.

`AWSAccountUsageReportAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAccountUsageReportAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountUsageReportAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewUsage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAgentlessDiscoveryService

Descrição: Fornece acesso para que o Discovery Agentless Connector se registre no AWS Application Discovery Service.

`AWSAgentlessDiscoveryService` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAgentlessDiscoveryService` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 02 de agosto de 2016, 1:35 UTC
- Hora da edição: 24 de fevereiro de 2020, 23:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "awsconnector:RegisterConnector",
        "awsconnector:GetConnectorHealth"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::connector-platform-upgrade-info/*",
        "arn:aws:s3:::connector-platform-upgrade-info",
        "arn:aws:s3:::connector-platform-upgrade-bundles/*",
        "arn:aws:s3:::connector-platform-upgrade-bundles",
        "arn:aws:s3:::connector-platform-release-notes/*",
        "arn:aws:s3:::connector-platform-release-notes",
        "arn:aws:s3:::prod.agentless.discovery.connector.upgrade/*",
        "arn:aws:s3:::prod.agentless.discovery.connector.upgrade"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::import-to-ec2-connector-debug-logs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    },
    {
      "Sid" : "Discovery",
      "Effect" : "Allow",
      "Action" : [
        "Discovery:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "arsenal",
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAgentRegistryServiceRolePolicy

Descrição: permite que o AWS Agent Registry acesse os recursos do AWS serviço em seu nome

`AWSAgentRegistryServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 06 de agosto de 2026, 14:27 UTC
- Horário editado: 21 de agosto de 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAgentRegistryServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOrganizationsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowSLRCreationForAWSConfig",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowConfigRecorderWrite",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:PutServiceLinkedConfigurationRecorder"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "config:ConfigurationRecorderServicePrincipal" : [
            "agent-registry.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowConfigRecorderRead",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForAgentRegistry*"
      ]
    },
```

```
    {
      "Sid" : "AllowRegistryRecordReadWrite",
      "Effect" : "Allow",
      "Action" : [
        "agent-registry:CreateRegistryRecord",
        "agent-registry:DeleteRegistryRecord",
        "agent-registry:GetRegistryRecord",
        "agent-registry:ListRegistryRecords",
        "agent-registry:UpdateRegistryRecord"
      ],
      "Resource" : [
        "arn:aws:agent-registry:*:*:registry/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPublishCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/AgentRegistry",
            "AWS/Usage"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppConfigServiceRolePolicy

Descrição: Permite ligar AWS AppConfig para AWS os serviços em seu nome.

`AWSAppConfigServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 08 de maio de 2026, 18:42 UTC
- Horário editado: 08 de maio de 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppConfigServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchPutExperimentMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AppConfig"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppFabricFullAccess

Descrição: fornece acesso total ao AWS AppFabric serviço e acesso somente para leitura a serviços dependentes, como S3, Kinesis e KMS.

`AWSAppFabricFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAppFabricFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de junho de 2023, 19:51 UTC
- Hora da edição: 27 de junho de 2023, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appfabric:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FirehoseReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowUseOfServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "appfabric.amazonaws.com"
        }
      },
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appfabric.amazonaws.com/
AWSServiceRoleForAppFabric"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppFabricReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao AWS AppFabric

`AWSAppFabricReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAppFabricReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de junho de 2023, 19:52 UTC
- Hora da edição: 27 de junho de 2023, 19:52 UTC

- ARN: `arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appfabric:GetAppAuthorization",
        "appfabric:GetAppBundle",
        "appfabric:GetIngestion",
        "appfabric:GetIngestionDestination",
        "appfabric:ListAppAuthorizations",
        "appfabric:ListAppBundles",
        "appfabric:ListIngestionDestinations",
        "appfabric:ListIngestions",
        "appfabric:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppFabricServiceRolePolicy

Descrição: Fornece AppFabric acesso a AWS recursos em seu nome

`AWSAppFabricServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 26 de junho de 2023, 21:07 UTC
- Hora da edição: 26 de junho de 2023, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEmitMetric",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AppFabric"
        }
      }
    },
    {
      "Sid" : "S3PutObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*/AWSAppFabric/*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FirehosePutRecord",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/AWSAppFabricManaged" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationAutoscalingAppStreamFleetPolicy

Descrição: Política que concede permissões ao Application Auto Scaling para acessar e. AppStream CloudWatch

`AWSApplicationAutoscalingAppStreamFleetPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 20 de outubro de 2017, 19:04 UTC
- Hora da edição: 20 de outubro de 2017, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationAutoscalingCassandraTablePolicy

Descrição: Política que concede permissões ao Application Auto Scaling para acessar Cassandra e. CloudWatch

`AWSApplicationAutoscalingCassandraTablePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 18 de março de 2020, 22:49 UTC
- Hora da edição: 18 de março de 2020, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cassandra:Select",
      "Resource" : [
        "arn:*:cassandra:*:*:/keyspace/system/table/*",
        "arn:*:cassandra:*:*:/keyspace/system_schema/table/*",
        "arn:*:cassandra:*:*:/keyspace/system_schema_mcs/table/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Alter",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationAutoscalingComprehendEndpointPolicy

Descrição: Política que concede permissões ao Application Auto Scaling para acessar o Comprehend e. CloudWatch

`AWSApplicationAutoscalingComprehendEndpointPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 14 de novembro de 2019, 18:39 UTC
- Hora da edição: 14 de novembro de 2019, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationAutoScalingCustomResourcePolicy

Descrição: Política que concede permissões ao Application Auto Scaling para acessar o ApiGateway e para escalonamento personalizado de recursos CloudWatch

`AWSApplicationAutoScalingCustomResourcePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 04 de junho de 2018, 23:22 UTC
- Hora da edição: 04 de junho de 2018, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationAutoscalingDynamoDBTablePolicy

Descrição: Política que concede permissões ao Application Auto Scaling para acessar o DynamoDB e. CloudWatch

`AWSApplicationAutoscalingDynamoDBTablePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 20 de outubro de 2017, 21:34 UTC
- Hora da edição: 20 de outubro de 2017, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

Descrição: Política que concede permissões ao Application Auto Scaling para acessar o EC2 Spot Fleet e. CloudWatch

`AWSApplicationAutoscalingEC2SpotFleetRequestPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 25 de outubro de 2017, 18:23 UTC
- Hora da edição: 25 de outubro de 2017, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationAutoscalingECSServicePolicy

Descrição: Política que concede permissões ao Application Auto Scaling para acessar o EC2 Container Service e. CloudWatch

`AWSApplicationAutoscalingECSServicePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 25 de outubro de 2017, 23:53 UTC
- Horário editado: 20 de maio de 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:DescribeServiceRevisions",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationAutoscalingElastiCacheRGPolicy

Descrição: Política que concede permissões ao Application Auto Scaling para acessar a Amazon ElastiCache e a Amazon. CloudWatch

`AWSApplicationAutoscalingElastiCacheRGPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 17 de agosto de 2021, 23:41 UTC
- Horário editado: 26 de março de 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "ElastiCacheActionsOnAllClusters",
      "Effect" : "Allow",
      "Action" : [
        "elasticache:DescribeReplicationGroups",
        "elasticache:ModifyCacheCluster",
        "elasticache:ModifyReplicationGroupShardConfiguration",
        "elasticache:IncreaseReplicaCount",
        "elasticache:DecreaseReplicaCount",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameters"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchActionsOnAllAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Sid" : "CloudWatchActionsOnTargetTrackingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationAutoscalingEMRInstanceGroupPolicy

Descrição: Política que concede permissões ao Application Auto Scaling para acessar o Elastic Map Reduce e. CloudWatch

`AWSApplicationAutoscalingEMRInstanceGroupPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 26 de outubro de 2017, 0:57 UTC
- Hora da edição: 26 de outubro de 2017, 0:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationAutoscalingKafkaClusterPolicy

Descrição: Política que concede permissões ao Application Auto Scaling para acessar o Managed Streaming para Apache Kafka e. CloudWatch

`AWSApplicationAutoscalingKafkaClusterPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 24 de agosto de 2020, 18:36 UTC
- Hora da edição: 24 de agosto de 2020, 18:36 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationAutoscalingLambdaConcurrencyPolicy

Descrição: Política que concede permissões ao Application Auto Scaling para acessar o Lambda e. CloudWatch

`AWSApplicationAutoscalingLambdaConcurrencyPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 21 de outubro de 2019, 20:04 UTC
- Hora da edição: 21 de outubro de 2019, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationAutoscalingNeptuneClusterPolicy

Descrição: Política que concede permissões ao Application Auto Scaling para acessar o Amazon Neptune e a Amazon. CloudWatch

`AWSApplicationAutoscalingNeptuneClusterPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 02 de setembro de 2021, 21:14 UTC
- Hora da edição: 02 de setembro de 2021, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterParameters",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:AddTagsToResource",
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : "neptune"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:CreateDBInstance",
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*",
```

```
        "arn:aws:rds:*:*:cluster:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : "neptune"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationAutoscalingRDSClusterPolicy

Descrição: Política que concede permissões ao Application Auto Scaling para acessar o RDS e. CloudWatch

`AWSApplicationAutoscalingRDSClusterPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 17 de outubro de 2017, 17:46 UTC
- Hora da edição: 07 de agosto de 2018, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CreateDBInstance",
        "rds:DeleteDBInstance",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "rds:ModifyDBCluster",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "rds.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationAutoscalingSageMakerEndpointPolicy

Descrição: Política que concede permissões ao Application Auto Scaling para acessar e. SageMaker CloudWatch

`AWSApplicationAutoscalingSageMakerEndpointPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Hora da criação: 06 de fevereiro de 2018, 19:58 UTC
- Hora da edição: 13 de novembro de 2023, 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMaker",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SageMakerCloudWatchUpdate",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
```

```
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationAutoscalingWorkSpacesPoolPolicy

Descrição: Política que concede permissões ao Application Auto Scaling para acessar a Amazon WorkSpaces e a Amazon. CloudWatch

`AWSApplicationAutoscalingWorkSpacesPoolPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 17 de junho de 2024, 18:39 UTC
- Hora da edição: 17 de junho de 2024, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingWorkSpacesPoolPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkSpacesActionsOnAllPools",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeWorkspacesPools",
        "workspaces:UpdateWorkspacesPool"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchActionsOnAllAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchActionsOnTargetTrackingAlarms",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationDiscoveryAgentAccess

Descrição: Fornece acesso para que o Discovery Agent se registre no AWS Application Discovery Service.

`AWSApplicationDiscoveryAgentAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationDiscoveryAgentAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de maio de 2016, 21:38 UTC
- Hora da edição: 24 de fevereiro de 2020, 22:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationDiscoveryAgentlessCollectorAccess

Descrição: permite que os coletores sem agente do Application Discovery Service atualizem, registrem e se comuniquem automaticamente com o Application Discovery Service

`AWSApplicationDiscoveryAgentlessCollectorAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationDiscoveryAgentlessCollectorAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 16 de agosto de 2022, 21:00 UTC
- Hora da edição: 16 de agosto de 2022, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:DescribeImages"
      ],
      "Resource" : "arn:aws:ecr-
public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sts:GetServiceBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationDiscoveryServiceFullAccess

Descrição: Fornece acesso total para visualizar e marcar itens de configuração mantidos pelo AWS Application Discovery Service

`AWSApplicationDiscoveryServiceFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationDiscoveryServiceFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de maio de 2016, 21:30 UTC
- Hora da edição: 19 de junho de 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:*",
        "discovery:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
```

```
    {
      "Action" : [
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "migrationhub.amazonaws.com",
            "dmsintegration.migrationhub.amazonaws.com",
            "smsintegration.migrationhub.amazonaws.com"
          ]
        }
      }
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationMigrationAgentInstallationPolicy

Descrição: Essa política permite instalar o Agente de AWS Replicação, que é usado com o Serviço de Migração de AWS Aplicativos (MGN) para migrar servidores externos para o. AWS Anexe essa política aos seus usuários ou funções do IAM cujas credenciais você fornece ao instalar o Agente de AWS Replicação.

`AWSApplicationMigrationAgentInstallationPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationMigrationAgentInstallationPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 19 de junho de 2022, 7:51 UTC
- Hora da edição: 20 de setembro de 2022, 11:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:VerifyClientRoleForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:IssueClientCertificateForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "mgn:CreateAction" : "RegisterAgentForMgn"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationMigrationAgentPolicy

Descrição: Essa política permite instalar e usar o Agente de AWS Replicação, que é usado com o Serviço de Migração de AWS Aplicativos (MGN) para migrar servidores externos para o. AWS Anexe essa política aos seus usuários ou funções do IAM cujas credenciais você fornece ao instalar o Agente de AWS Replicação.

`AWSApplicationMigrationAgentPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationMigrationAgentPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 7 de abril de 2021, 7:00 UTC
- Hora da edição: 20 de setembro de 2022, 11:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:RegisterAgentForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationMigrationAgentPolicy_v2

Descrição: Essa política permite usar o Agente de AWS Replicação, que é usado com o Serviço de Migração de AWS Aplicativos (MGN) para migrar servidores externos para o. AWS Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM.

`AWSApplicationMigrationAgentPolicy_v2` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationMigrationAgentPolicy_v2` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 06 de junho de 2022, 14:14 UTC
- Hora da edição: 06 de junho de 2022, 14:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn",
        "mgn:IssueClientCertificateForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/${aws:SourceIdentity}"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationMigrationConversionServerPolicy

Descrição: esta política permite que o servidor de conversão do Application Migration Service (MGN), que são instâncias do EC2 iniciadas pelo Application Migration Service, se comunique com o serviço MGN. Uma função do IAM com essa política é anexada (como um perfil de instância do EC2) pela MGN aos servidores de conversão da MGN, que são iniciados e encerrados automaticamente pela MGN, quando necessário. Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM. Os servidores de conversão MGN são usados pelo Application Migration Service quando os usuários optam por iniciar instâncias de teste ou transferência usando o console, a CLI ou a API do MGN.

`AWSApplicationMigrationConversionServerPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationMigrationConversionServerPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 7 de abril de 2021, 6:48 UTC
- Hora da edição: 7 de abril de 2021, 6:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationMigrationEC2Access

Descrição: esta política fornece ao Amazon EC2 as operações necessárias para usar o Application Migration Service (MGN) para iniciar os servidores migrados como instâncias do EC2. Anexe essa política aos seus usuários ou funções do IAM.

`AWSApplicationMigrationEC2Access` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationMigrationEC2Access` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 7 de abril de 2021, 7:05 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
```

```
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:ModifyVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationMigrationFSxProxyPolicy

Descrição: Fornece permissões para gerenciar o sistema de arquivos ONTAP

`AWSApplicationMigrationFSxProxyPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationMigrationFSxProxyPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 31 de maio de 2026, 13:12 UTC
- Horário editado: 09 de agosto de 2026, 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationFSxProxyPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FSxSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxDescribe",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeVolumes",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FSxCreateVolume",
      "Effect" : "Allow",
      "Action" : "fsx:CreateVolume",
      "Resource" : "arn:aws:fsx:*:*:volume/*/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxCreateVolumeSVM",
      "Effect" : "Allow",
      "Action" : "fsx:CreateVolume",
      "Resource" : "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
    },
```

```
    {
      "Sid" : "FSxTagging",
      "Effect" : "Allow",
      "Action" : [
        "fsx:TagResource",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxUpdateAndDeleteVolume",
      "Effect" : "Allow",
      "Action" : [
        "fsx:UpdateVolume",
        "fsx:DeleteVolume"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxCreateSnapshot",
      "Effect" : "Allow",
      "Action" : "fsx:CreateSnapshot",
      "Resource" : "arn:aws:fsx:*:*:snapshot/*/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxCreateSnapshotVolume",
      "Effect" : "Allow",
      "Action" : "fsx:CreateSnapshot",
      "Resource" : "arn:aws:fsx:*:*:volume/*/*",
```

```
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxDeleteSnapshot",
      "Effect" : "Allow",
      "Action" : "fsx:DeleteSnapshot",
      "Resource" : "arn:aws:fsx:*:*:snapshot/*/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxTagSnapshot",
      "Effect" : "Allow",
      "Action" : "fsx:TagResource",
      "Resource" : "arn:aws:fsx:*:*:snapshot/*/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationMigrationFSxProxyVPCPolicy

Descrição: Fornece permissões para gerenciar PrivateLink entre o AWS Application Migration Service e o sistema de arquivos FSx do cliente

`AWSApplicationMigrationFSxProxyVPCPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationMigrationFSxProxyVPCPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 31 de maio de 2026, 13:27 UTC
- Horário editado: 31 de maio de 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationFSxProxyVPCPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowlistAllVPCsforSGCreation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
```

```
    {
      "Sid" : "CreateServiceEndpointResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc-endpoint-service/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/file_system_id" : "false",
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "EC2AllowOperationsOnTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVpcEndpointServiceConfigurations"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc-endpoint-service/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/file_system_id" : "false",
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:GetSecurityGroupsForVpc",
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "ec2:DescribeInternetGateways",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModifyVpcEndpointOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:AcceptVpcEndpointConnections"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint-service/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/file_system_id" : "false",
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "EC2AllowTaggingOnCreate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc-endpoint-service/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVpcEndpointServiceConfiguration"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "CreateFSxNLB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/MgnFSxProxy*NLB/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/MgnFSxProxy*/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/file_system_id" : "false",
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "FSxNLBAllowTaggingOnCreate",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:AddTags",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/MgnFSxProxy*NLB/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/MgnFSxProxy*TG/*",
        "arn:aws:elasticloadbalancing:*:*:listener/net/MgnFSxProxy*/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer",
            "CreateTargetGroup",
            "CreateListener"
          ]
        }
      }
    },
    {
      "Sid" : "FSxNLBRole",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "RegisterFSxTargetGroup",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:RegisterTargets",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/MgnFSxProxy*/*"
    },
    {
      "Sid" : "ELBv2AllowModify",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyLoadBalancerAttributes",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/MgnFSxProxy*/*"
    },
    {
      "Sid" : "ELBv2AllowOperationsOnTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/MgnFSxProxy*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/net/MgnFSxProxy*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/MgnFSxProxy*/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/file_system_id" : "false",
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationMigrationFullAccess

Descrição: Essa política fornece permissões para todas as APIs públicas do AWS Application Migration Service (MGN), bem como permissões para ler as principais informações do KMS. Anexe essa política aos seus usuários ou funções do IAM.

`AWSApplicationMigrationFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationMigrationFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 7 de abril de 2021, 6:56 UTC
- Horário editado: 03 de agosto de 2026, 10:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess`

Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "mgn:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor5",
      "Effect" : "Allow",
      "Action" : "iam:ListInstanceProfiles",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor6",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole",
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithDrsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "VisualEditor7",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "VisualEditor9",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor10",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "VisualEditor11",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "VisualEditor12",
      "Effect" : "Allow",
      "Action" : [
        "drs:DisconnectSourceServer"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceConfiguredDR" : "false"
        }
      }
    },
    {
      "Sid" : "VisualEditor13",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
```

```
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
    },
    {
      "Sid" : "VisualEditor14",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor15",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*"
    },
    {
      "Sid" : "VisualEditor16",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ]
    },
    {
      "Sid" : "VisualEditor17",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "VisualEditor18",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSMigration-*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSMigration-*:$DEFAULT"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "mgn.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor19",
      "Effect" : "Allow",
      "Action" : "ssm:ListCommands",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor20",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeParameters"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "FSxReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowTagSVMWithMapKeys",
      "Effect" : "Allow",
      "Action" : [
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:storage-virtual-machine/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "map-migrated",
            "aws-apn-id"
          ]
        }
      }
    },
    {
      "Sid" : "FSxDescribeOperations",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeVolumes",
        "fsx:DescribeSnapshots"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FSxCreateVolume",
      "Effect" : "Allow",
```

```
      "Action" : "fsx:CreateVolume",
      "Resource" : [
        "arn:aws:fsx:*:*:volume/*/*",
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FSxDeleteVolumeAndTag",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteVolume",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FSxCreateSnapshot",
      "Effect" : "Allow",
      "Action" : "fsx:CreateSnapshot",
      "Resource" : [
        "arn:aws:fsx:*:*:snapshot/*/*",
        "arn:aws:fsx:*:*:volume/*/*"
      ],
      "Condition" : {
```

```
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationMigrationMGHAccess

Descrição: Essa política permite que o AWS Application Migration Service (MGN) envie metadados sobre o progresso dos servidores que estão sendo migrados usando o MGN para o AWS Migration Hub (MGH). A MGN cria automaticamente uma função do IAM com essa política anexada e assume essa função. Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM.

`AWSApplicationMigrationMGHAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationMigrationMGHAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 7 de abril de 2021, 7:10 UTC

- Hora da edição: 7 de abril de 2021, 7:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationMigrationNetworkMigrationCustomResource

Descrição: Fornece permissões para o recurso personalizado de migração de rede

`AWSApplicationMigrationNetworkMigrationCustomResource` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationMigrationNetworkMigrationCustomResource` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 05 de novembro de 2025, 11:34 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationNetworkMigrationCustomResource`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ModifyTGW",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyTransitGateway"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationMigrationNetworkMigrationMultiAccount

Descrição: Fornece permissões para automatizar a migração da VMware para a infraestrutura de AWS rede por meio de CloudFormation

`AWSApplicationMigrationNetworkMigrationMultiAccount` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationMigrationNetworkMigrationMultiAccount` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Tempo de criação: 10 de novembro de 2025, 09:04 UTC
- Horário editado: 15 de setembro de 2026, 13:17 UTC

- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationNetworkMigrationMultiAccount`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2CFNReadonlyPrefixList",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:prefix-list/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "NetworkAnalyzer",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreatePermissionsByCFNNACL",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByCFNNACLSN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
```

```
      "Sid" : "EC2CFNReadonly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetTransitGatewayRouteTableAssociations",
```

```
        "ec2:GetTransitGatewayRouteTablePropagations"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "MGNCFNDescribe",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*"
    },
    {
      "Sid" : "CFNCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CFNTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
```

```
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack"
          ]
        }
      }
    },
    {
      "Sid" : "CFNOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CFNProvision",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
```

```
      "Sid" : "AnalyzerEC2PutResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2ResourceOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2ResourceSgTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2RequestSgTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2SecurityGroupTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "EC2TagCFNSG",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByCFN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
```

```
        "ec2:CreateNatGateway",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInsightsPath"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AllowCreateTGWVpcAttachmentSameOrg",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*"
      ],
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        }
      }
    },
    {
      "Sid" : "CFNProvisionNetworking",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateVpc",
        "ec2:CreateTransitGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:transit-gateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagNetworking",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAcl",
        "ec2:CreateSubnet",
        "ec2:CreateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagRouting",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagNAT",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagTransitGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagTGWAttachment",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "DeleteENI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagInsights",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateNetworkInsightsPath"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-insights-path/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "EC2TagCFN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-policy-table/*",
        "arn:aws:ec2:*:*:transit-gateway-connect-peer/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:network-insights-access-scope-analysis/*",
        "arn:aws:ec2:*:*:network-insights-access-scope/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:network-insights-analysis/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "ec2:CreateAction" : [
            "CreateTransitGatewayVpcAttachment",
            "CreateTransitGatewayRouteTableAnnouncement",
            "CreateTransitGatewayRouteTable",
            "CreateTransitGatewayRoute",
            "CreateTransitGatewayPrefixListReference",
            "CreateTransitGatewayPolicyTable",
            "CreateTransitGatewayPeeringAttachment",
            "CreateTransitGatewayConnectPeer",
            "CreateTransitGatewayConnect",
            "CreateTransitGateway",
            "CreateInternetGateway",
            "CreateNatGateway",
            "CreateSubnet",
            "CreateNetworkAcl",
            "CreateRouteTable",
            "CreateNetworkInterface",
            "CreateNetworkInsightsPath",
            "CreateNetworkInsightsAccessScope",
            "CreateLaunchTemplate",
            "AllocateAddress",
            "StartNetworkInsightsAnalysis",
            "CreateVpc"
          ]
        }
      }
    },
    {
      "Sid" : "deployerWorkload",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "putParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "deleteParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:DeleteResourcePolicy",
        "ssm:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
```

```
      }
    },
    {
      "Sid" : "ramResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutResourcePolicy",
        "ssm:GetResourcePolicies"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ramTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreateResourceShareTransitGateway",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
```

```
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "Bool" : {
          "ram:RequestedAllowsExternalPrincipals" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AssociateResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService",
          "ram:RequestedResourceType" : [
            "ec2:TransitGateway",
            "ssm:Parameter"
          ]
        }
      }
    },
    {
      "Sid" : "CreateResourceShareWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:DisassociateResourceShare",
```

```
        "ram:UpdateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AllowGetResourceShares",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*"
    },
    {
      "Sid" : "CreateCustomResourceLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/network-migration-modify-tgw*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateCustomResourceLambda",
      "Effect" : "Allow",
```

```
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "GetCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:ListTags"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OperationsCustomResourceLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
```

```
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreateRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "PassGetRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OperationsRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
```

```
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AttachCustomResourceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole",
            "arn:aws:iam::aws:policy/
AWSApplicationMigrationNetworkMigrationCustomResource"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "MGNCFNBasedResourcesProvision",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptTransitGatewayVpcAttachment",
        "ec2:AssociateNatGatewayAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteInternetGateway",
```

```
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteSubnet",
        "ec2:DeleteTransitGateway",
        "ec2:DeleteTransitGatewayRoute",
        "ec2:DeleteTransitGatewayRouteTable",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DisableTransitGatewayRouteTablePropagation",
        "ec2:DisassociateNatGatewayAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyLaunchTemplate",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyTransitGateway",
        "ec2:ModifyTransitGatewayVpcAttachment",
        "ec2:ModifyVolume",
        "ec2:ModifyVpcAttribute",
        "ec2:RejectTransitGatewayVpcAttachment",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceTransitGatewayRoute",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-policy-table/*",
        "arn:aws:ec2:*:*:transit-gateway-connect-peer/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:network-insights-access-scope-analysis/*",
        "arn:aws:ec2:*:*:network-insights-access-scope/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:network-insights-analysis/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreateTransitGatewaySLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/aws-service-role/transitgateway.amazonaws.com/
AWSServiceRoleForVPCTransitGateway"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "transitgateway.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AnalyzerENIResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationMigrationReadOnlyAccess

Descrição: Essa política fornece permissões para todas as APIs públicas somente para leitura do Application Migration Service (MGN), bem como para algumas APIs somente para leitura de outros

AWS serviços que são necessárias para fazer uso completo do console MGN somente para leitura. Anexe essa política aos seus usuários ou funções do IAM.

`AWSApplicationMigrationReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationMigrationReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 7 de abril de 2021, 7:15 UTC
- Horário editado: 01 de julho de 2026, 14:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeSourceServers",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:GetLaunchConfiguration",
        "mgn:DescribeVcenterClients",
        "mgn:GetReplicationConfiguration",
```

```
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListApplications",
        "mgn:ListWaves",
        "mgn:ListExports",
        "mgn:ListImports",
        "mgn:ListImportErrors",
        "mgn:ListExportErrors"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationMigrationReplicationServerPolicy

Descrição: Essa política permite que os servidores de replicação do Serviço de Migração de Aplicativos (MGN), que são instâncias do EC2 iniciadas pelo Serviço de Migração de Aplicativos, se comuniquem com o serviço MGN e criem instantâneos do EBS em seu. Conta da AWS Uma função do IAM com essa política é anexada (como um perfil de instância do EC2) pelo Application Migration Service aos servidores de replicação da MGN, que são automaticamente iniciados e encerrados pela MGN, conforme necessário. Os servidores de replicação MGN são usados para facilitar a replicação de dados de seus servidores externos para AWS, como parte do processo de migração gerenciado usando o MGN. Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM.

`AWSApplicationMigrationReplicationServerPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationMigrationReplicationServerPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 7 de abril de 2021, 7:21 UTC
- Horário editado: 31 de maio de 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn",
        "mgn:GetAgentSnapshotCreditsForMgn",
        "mgn:DescribeReplicationServerAssociationsForMgn",
        "mgn:DescribeSnapshotRequestsForMgn",
        "mgn:BatchDeleteSnapshotRequestForMgn",
        "mgn:NotifyAgentAuthenticationForMgn",
        "mgn:BatchCreateVolumeSnapshotGroupForMgn",
        "mgn:UpdateAgentReplicationProcessStateForMgn",
        "mgn:NotifyAgentReplicationProgressForMgn",
        "mgn:NotifyAgentConnectedForMgn",
        "mgn:NotifyAgentDisconnectedForMgn",
        "mgn:StartSnapshotGroupForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationMigrationServiceEc2InstancePolicy

Descrição: Essa política permite instalar e usar o Agente de AWS Replicação, que é usado pelo AWS Application Migration Service (AWS MGN) para migrar servidores de origem executados no

EC2 (entre regiões ou cross-AZ). Uma função do IAM com essa política deve ser anexada (como um perfil de instância do EC2) às instâncias do EC2.

`AWSApplicationMigrationServiceEc2InstancePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationMigrationServiceEc2InstancePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 22 de agosto de 2023, 13:19 UTC
- Hora da edição: 3 de janeiro de 2024, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MgnAgentInstallation",
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:GetAgentInstallationAssetsForMgn"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MgnAgentReplication",
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    },
    {
      "Sid" : "MgnSourceServerTagResource",
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "mgn:CreateAction" : "RegisterAgentForMgn"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationMigrationServiceRolePolicy

Descrição: permite que o serviço de migração de AWS aplicativos crie e gerencie AWS recursos em seu nome.

`AWSApplicationMigrationServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 7 de abril de 2021, 6:43 UTC
- Horário editado: 19 de julho de 2026, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgn:ListTagsForResource",
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
```

```
      "Resource" : "arn:aws:organizations::*:account/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
```

```
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
```

```
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationReplicationServerRole",
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "RegisterImage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationMigrationSSMAccess

Descrição: esta política fornece acesso às operações do Amazon SSM necessárias para usar o Application Migration Service (MGN) para executar documentos do SSM de comandos pós-migração personalizados. Anexe essa política aos seus usuários ou funções do IAM.

`AWSApplicationMigrationSSMAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationMigrationSSMAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de novembro de 2022, 9:29 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocumentVersions",
        "ssm:GetDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSApplicationMigrationVCenterClientPolicy

Descrição: Essa política permite instalar e usar o AWS vCenter Client, que é usado com o AWS Application Migration Service (MGN) para migrar servidores externos para o. AWS Anexe essa política aos seus usuários ou funções do IAM cujas credenciais você fornece ao instalar o AWS vCenter Client.

`AWSApplicationMigrationVCenterClientPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSApplicationMigrationVCenterClientPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de novembro de 2021, 12:53 UTC
- Hora da edição: 08 de novembro de 2021, 12:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:CreateVcenterClientForMgn",
        "mgn:DescribeVcenterClients"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetVcenterClientCommandsForMgn",
        "mgn:SendVcenterClientCommandResultForMgn",
        "mgn:SendVcenterClientLogsForMgn",
        "mgn:SendVcenterClientMetricsForMgn",
        "mgn:DeleteVcenterClient",
        "mgn:TagResource",
        "mgn:NotifyVcenterClientStartedForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:vcenter-client/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppMeshEnvoyAccess

Descrição: política do App Mesh Envoy para acessar a configuração de nó virtual.

`AWSAppMeshEnvoyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAppMeshEnvoyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 03 de julho de 2019, 21:29 UTC

- Hora da edição: 03 de julho de 2019, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh:StreamAggregatedResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppMeshFullAccess

Descrição: fornece acesso total às APIs do AWS App Mesh e ao console de gerenciamento.

`AWSAppMeshFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAppMeshFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 16 de abril de 2019, 17:50 UTC
- Hora da edição: 07 de janeiro de 2021, 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshFullAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appmesh.amazonaws.com/
AWSServiceRoleForAppMesh",
      "Condition" : {
```

```
        "StringLike" : {
          "iam:AWSServiceName" : [
            "appmesh.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStack*",
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSAppMesh-GettingStarted-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "acm:DescribeCertificate",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppMeshPreviewEnvoyAccess

Descrição: política do App Mesh Preview Envoy para acessar a configuração de nó virtual.

`AWSAppMeshPreviewEnvoyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAppMeshPreviewEnvoyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 05 de agosto de 2019, 23:32 UTC
- Hora da edição: 05 de agosto de 2019, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh-preview:StreamAggregatedResources"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppMeshPreviewServiceRolePolicy

Descrição: permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo AWS App Mesh

`AWSAppMeshPreviewServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 19 de junho de 2019, 19:07 UTC
- Hora da edição: 21 de agosto de 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppMeshReadOnly

Descrição: fornece acesso somente para leitura às APIs do AWS App Mesh e ao console de gerenciamento.

`AWSAppMeshReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAppMeshReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 16 de abril de 2019, 17:51 UTC
- Hora da edição: 07 de janeiro de 2021, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshReadOnly`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh:Describe*",
        "appmesh:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSAppMesh-GettingStarted-*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "acm:DescribeCertificate",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppMeshServiceRolePolicy

Descrição: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados por AWS AppMesh

`AWSAppMeshServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 03 de junho de 2019, 18:30 UTC
- Hora da edição: 10 de outubro de 2023, 16:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppRunnerFullAccess

Descrição: concede permissões a todas as ações do App Runner.

`AWSAppRunnerFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAppRunnerFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de janeiro de 2022, 4:02 UTC
- Hora da edição: 11 de janeiro de 2022, 4:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/apprunner.amazonaws.com/
AWSServiceRoleForAppRunner",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "apprunner.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "apprunner.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRunnerAdminAccess",
      "Effect" : "Allow",
      "Action" : "apprunner:*",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppRunnerReadOnlyAccess

Descrição: concede permissões para listar e visualizar detalhes dos recursos do App Runner.

`AWSAppRunnerReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAppRunnerReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de fevereiro de 2022, 21:24 UTC
- Hora da edição: 24 de fevereiro de 2022, 21:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apprunner:List*",
        "apprunner:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppRunnerServicePolicyForECRAccess

Descrição: Política de serviço do AWS App Runner que concede permissões de leitura aos recursos do Amazon ECR na conta do cliente. Use-o em uma função que é passada para o App Runner ao criar ou atualizar um serviço do App Runner.

`AWSAppRunnerServicePolicyForECRAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAppRunnerServicePolicyForECRAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 14 de maio de 2021, 19:17 UTC
- Hora da edição: 14 de maio de 2021, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppSyncAdministrator

Descrição: Fornece acesso administrativo ao AppSync serviço, embora não seja suficiente para acessar por meio do console.

`AWSAppSyncAdministrator` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAppSyncAdministrator` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 20 de março de 2018, 21:20 UTC
- Hora da edição: 04 de novembro de 2019, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncAdministrator`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "appsync.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "appsync.amazonaws.com"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appsync.amazonaws.com/
AWSServiceRoleForAppSync*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppSyncInvokeFullAccess

Descrição: Fornece acesso de invocação completo ao AppSync serviço, tanto por meio do console quanto de forma independente

`AWSAppSyncInvokeFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAppSyncInvokeFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 20 de março de 2018, 21:21 UTC
- Hora da edição: 20 de março de 2018, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppSyncPushToCloudWatchLogs

Descrição: Permite AppSync enviar registros para a CloudWatch conta do usuário.

`AWSAppSyncPushToCloudWatchLogs` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAppSyncPushToCloudWatchLogs` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 09 de abril de 2018, 19:38 UTC
- Hora da edição: 09 de abril de 2018, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppSyncSchemaAuthor

Descrição: fornece acesso para criar, atualizar e consultar o esquema.

`AWSAppSyncSchemaAuthor` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAppSyncSchemaAuthor` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 20 de março de 2018, 21:21 UTC
- Hora da edição: 01 de fevereiro de 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "appsync:GraphQL",
        "appsync:CreateResolver",
        "appsync:CreateType",
        "appsync:DeleteResolver",
        "appsync:DeleteType",
        "appsync:GetResolver",
        "appsync:GetType",
        "appsync:GetDataSource",
        "appsync:GetSchemaCreationStatus",
        "appsync:GetIntrospectionSchema",
        "appsync:GetGraphqlApi",
        "appsync:ListTypes",
        "appsync:ListApiKeys",
        "appsync:ListResolvers",
        "appsync:ListDataSources",
        "appsync:ListGraphqlApis",
        "appsync:StartSchemaCreation",
        "appsync:UpdateResolver",
        "appsync:UpdateType",
        "appsync:TagResource",
        "appsync:UntagResource",
        "appsync:ListTagsForResource",
        "appsync:CreateFunction",
        "appsync:UpdateFunction",
        "appsync:GetFunction",
        "appsync:DeleteFunction",
        "appsync:ListFunctions",
        "appsync:ListResolversByFunction",
        "appsync:EvaluateMappingTemplate",
        "appsync:EvaluateCode"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAppSyncServiceRolePolicy

Descrição: Permite o acesso a AWS serviços e recursos usados ou gerenciados pelo AppSync

`AWSAppSyncServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário da criação: 21 de janeiro de 2020, 19:56 UTC
- Hora da edição: 21 de janeiro de 2020, 19:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
```

```
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSArtifactAccountSync

Descrição: Permite acesso somente para leitura do AWS Artifact às operações nas organizações. AWS

`AWSArtifactAccountSync` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSArtifactAccountSync` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 10 de abril de 2018, 23:04 UTC
- Hora da edição: 10 de abril de 2018, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSArtifactAgreementsFullAccess

Descrição: Essa política concede permissões completas para listar, baixar, aceitar e rescindir contratos do AWS Artifact. Também inclui permissões para listar e habilitar o acesso ao AWS serviço no serviço Organização, bem como descrever os detalhes da organização. Além disso, a política fornece a capacidade de verificar se a função necessária vinculada ao serviço existe e, caso não exista, cria uma função.

`AWSArtifactAgreementsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSArtifactAgreementsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 22 de novembro de 2024, 19:36 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactAgreementsFullAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource" : "arn:aws:artifact:::agreement/*"
    },
```

```
    {
      "Sid" : "CustomerAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource" : "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetRoleToCheckForRoleExistence",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid" : "EnableServiceTrust",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "EnableServiceTrustForArtifact",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "aws-artifact-account-sync.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSArtifactAgreementsReadOnlyAccess

Descrição: Essa política concede acesso somente para leitura para listar os contratos de serviço do AWS Artifact e baixar os contratos aceitos. Ela também inclui permissões para listar e descrever os detalhes da organização. Além disso, a política concede a capacidade de verificar se a função vinculada ao serviço necessária existe.

`AWSArtifactAgreementsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSArtifactAgreementsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 22 de novembro de 2024, 19:36 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactAgreementsReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListAgreementsActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetCustomerAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetCustomerAgreement"
      ],
      "Resource" : "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid" : "AWSOrganizationActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSArtifactComplianceInquiriesFullAccess

Descrição: Fornece acesso total ao Artifact Compliance Inquiry.

`AWSArtifactComplianceInquiriesFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSArtifactComplianceInquiriesFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Horário de criação: 30 de junho de 2026, 19:27 UTC
- Horário editado: 30 de setembro de 2026, 22:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactComplianceInquiriesFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListAndCreateComplianceInquiryActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListComplianceInquiries",
        "artifact:CreateComplianceInquiry"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ComplianceInquiryActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListComplianceInquiryQueries",
        "artifact:GetComplianceInquiryMetadata",
        "artifact:ExportComplianceInquiry",
        "artifact:PutComplianceInquiryFeedback"
      ],
      "Resource" : "arn:aws:artifact:*:*:compliance-inquiry/*"
    },
    {
      "Sid" : "NotificationConfigurationListActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "notifications:ListNotificationConfigurations",
        "notifications:ListChannels",
        "notifications:ListEventRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NotificationConfigurationContactReadActions",
      "Effect" : "Allow",
      "Action" : [
        "notifications-contacts:GetEmailContact"
      ],
      "Resource" : "arn:aws:notifications-contacts::*:emailcontact/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSArtifactComplianceInquiriesReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Artifact Compliance Inquiry.

`AWSArtifactComplianceInquiriesReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSArtifactComplianceInquiriesReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 30 de junho de 2026, 19:42 UTC

- Horário editado: 30 de junho de 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactComplianceInquiriesReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListComplianceInquiryActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListComplianceInquiries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetComplianceInquiryActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetComplianceInquiryMetadata",
        "artifact:ListComplianceInquiryQueries",
        "artifact:ExportComplianceInquiry"
      ],
      "Resource" : "arn:aws:artifact:*:*:compliance-inquiry/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSArtifactReportsReadOnlyAccess

Descrição: Fornece acesso somente para leitura aos relatórios do serviço AWS Artifact.

`AWSArtifactReportsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSArtifactReportsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 2 de janeiro de 2024, 22:42 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports",
        "artifact:ListReportVersions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSArtifactServiceRolePolicy

Descrição: permite que o AWS Artifact colete informações sobre uma organização por meio do serviço AWS Organizations.

`AWSArtifactServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 21 de agosto de 2023, 20:27 UTC
- Hora da edição: 21 de agosto de 2023, 20:27 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAuditManagerAdministratorAccess

Descrição: Fornece acesso administrativo para ativar ou desativar o AWS Audit Manager, atualizar configurações e gerenciar avaliações, controles e estruturas

`AWSAuditManagerAdministratorAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSAuditManagerAdministratorAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de dezembro de 2020, 20:02 UTC
- Hora da edição: 15 de maio de 2024, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AuditManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "auditmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
```

```
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOnlyAuditManagerIntegration",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "auditmanager.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
      "Condition" : {
        "StringLike" : {
```

```
          "iam:AWSServiceName" : "auditmanager.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMAccessManageSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:UpdateRoleDescription",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*"
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : "auditmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SNSAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.securityhub"
          ]
        }
      }
    },
    {
      "Sid" : "EventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
```

```
    },
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ControlCatalogAccess",
      "Effect" : "Allow",
      "Action" : [
        "controlcatalog:ListCommonControls",
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAuditManagerServiceRolePolicy

Descrição: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo AWS Audit Manager

`AWSAuditManagerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 08 de dezembro de 2020, 15:12 UTC
- Horário editado: 02 de junho de 2026, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:ListBackupPlans",
        "backup:ListRecoveryPointsByResource",
        "bedrock:GetCustomModel",
        "bedrock:GetFoundationModel",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListCustomModels",
```

```
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListModelCustomizationJobs",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListDistributions",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cognito-idp:DescribeUserPool",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:ListDiscoveredResources",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTable",
        "dynamodb:ListBackups",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:GetLaunchTemplateData",
        "ec2:DescribeAddresses",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
```

```
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ecs:DescribeClusters",
        "eks:DescribeAddonVersions",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeServiceUpdates",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSslPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListSecurityConfigurations",
        "events:DescribeRule",
        "events:ListConnections",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRules",
        "firehose:ListDeliveryStreams",
        "fsx:DescribeFileSystems",
        "guardduty:ListDetectors",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccessKeyLastUsed",
        "iam:GetCredentialReport",
        "iam:GetGroupPolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:ListAttachedGroupPolicies",
```

```
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupsForUser",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListOpenIdConnectProviders",
        "iam:ListPolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSamlProviders",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "iam:ListPolicyVersions",
        "iam:ListAccessKeys",
        "iam:ListAttachedRolePolicies",
        "iam:ListMfaDeviceTags",
        "iam:ListMfaDevices",
        "kafka:ListClusters",
        "kafka:ListKafkaVersions",
        "kinesis:ListStreams",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "lambda:ListFunctions",
        "license-manager:ListAssociationsForLicenseConfiguration",
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListUsageForLicenseConfiguration",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "es:DescribeDomains",
        "es:DescribeDomain",
        "es:DescribeDomainConfig",
        "es:ListDomainNames",
        "organizations:DescribeOrganization",
        "organizations:DescribePolicy",
```

```
        "organizations:DescribeAccount",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeLoggingStatus",
        "route53:GetQueryLoggingConfig",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListModels",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListUserProfiles",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketVersioning",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
```

```
        "s3:ListAllMyBuckets",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecrets",
        "securityhub:DescribeStandards",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:ListQueues",
        "waf-regional:GetRule",
        "waf-regional:GetWebAcl",
        "waf:GetRule",
        "waf:GetRuleGroup",
        "waf:ListActivatedRulesInRuleGroup",
        "waf:ListWebAcls",
        "wafv2:ListWebAcls",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:ListRuleGroups",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListWebACLs",
        "waf-regional:ListRules",
        "waf:ListRuleGroups",
        "waf:ListRules"
      ],
      "Resource" : "*",
      "Sid" : "APIsAccess"
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:GetBucketLogging",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported",
          "events:source" : [
            "aws.securityhub"
          ]
        },
        "Null" : {
          "events:source" : "false",
          "events:detail-type" : "false"
        }
      }
    },
    {
      "Sid" : "EventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
```

```
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSAutoScalingPlansEC2AutoScalingPolicy

Descrição: Política que concede permissões ao AWS Auto Scaling para prever periodicamente a capacidade e gerar ações de escalabilidade programadas para grupos de Auto Scaling em um plano de escalabilidade

`AWSAutoScalingPlansEC2AutoScalingPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 23 de agosto de 2018, 22:46 UTC
- Hora da edição: 23 de agosto de 2018, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupAccessPointOperatorAccess

Descrição: Essa política concede aos usuários permissões para criar e gerenciar pontos de acesso de backup para acessar dados de backup em pontos de recuperação por meio de pontos de acesso S3.

`AWSBackupAccessPointOperatorAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBackupAccessPointOperatorAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 06 de agosto de 2026, 16:12 UTC
- Horário editado: 06 de agosto de 2026, 16:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAccessPointOperatorAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateBackupAccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupAccessPoint"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*"
    },
    {
      "Sid" : "BackupAccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeBackupAccessPoint",
        "backup:DeleteBackupAccessPoint"
      ],
```

```
      "Resource" : "arn:aws:backup:*:*:accesspoint/*"
    },
    {
      "Sid" : "ListBackupAccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:ListBackupAccessPoints",
        "backup:ListBackupAccessPointsByResource",
        "backup:ListBackupAccessPointsByRecoveryPoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3AccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateAccessPoint",
        "s3:DeleteAccessPoint",
        "s3:GetAccessPoint",
        "s3:PutAccessPointPolicy"
      ],
      "Resource" : "arn:aws:s3:*:*:accesspoint/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DecryptKMSEncryptedDataByAWSBackup",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "backup.*.amazonaws.com",
          "kms:EncryptionContext:aws:backup:backup-vault" : "*"
        }
      }
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupAuditAccess

Descrição: Essa política concede permissões para que os usuários criem controles e estruturas que definam suas expectativas em relação aos recursos e atividades de AWS backup e auditem os recursos e as atividades de AWS backup em relação aos controles e estruturas definidos. Essa política concede permissões ao AWS Config e a serviços similares para descrever as expectativas do usuário ao realizar as auditorias. Essa política também concede permissões para entregar relatórios de auditoria ao S3 e serviços similares e permite que os usuários encontrem e abram seus relatórios de auditoria.

`AWSBackupAuditAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBackupAuditAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de agosto de 2021, 1:02 UTC
- Hora da edição: 10 de abril de 2023, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAuditAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateFramework",
        "backup:UpdateFramework",
        "backup:ListFrameworks",
        "backup:DescribeFramework",
        "backup:DeleteFramework",
        "backup:ListBackupPlans",
        "backup:ListBackupVaults",
        "backup:CreateReportPlan",
        "backup:UpdateReportPlan",
        "backup:ListReportPlans",
        "backup:DescribeReportPlan",
        "backup:DeleteReportPlan",
        "backup:StartReportJob",
        "backup:ListReportJobs",
        "backup:DescribeReportJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeComplianceByConfigRule"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:GetComplianceDetailsByConfigRule"
```

```
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupDataTransferAccess

Descrição: Essa política permite que o agente AWS Backint conclua a transferência de dados de backup com o plano AWS Backup Storage. Vincule essa política às funções assumidas pelas instâncias do EC2 que executam o SAP HANA com o agente Backint.

`AWSBackupDataTransferAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBackupDataTransferAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 10 de novembro de 2022, 22:48 UTC
- Hora da edição: 10 de novembro de 2022, 22:48 UTC

- ARN: `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:StartObject",
        "backup-storage:PutChunk",
        "backup-storage:GetChunk",
        "backup-storage:ListChunks",
        "backup-storage:ListObjects",
        "backup-storage:GetObjectMetadata",
        "backup-storage:NotifyObjectComplete"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupFullAccess

Descrição: Essa política é para administradores de backup, concedendo acesso total às operações de AWS backup, incluindo criar ou editar planos de backup, atribuir AWS recursos aos planos de backup, excluir backups e restaurar backups.

`AWSBackupFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBackupFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de novembro de 2019, 22:21 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupFullAccess`

Versão da política

Versão da política: v30 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AwsBackupStorageAllAccessPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "backup-storage:*",
      "Resource" : "*"
    },
    {
      "Sid" : "RdsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusters",
        "rds:describeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RdsDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBClusterSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DynamoDbPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDbDeleteBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EfsFileSystemPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "Ec2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:describeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
```

```
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2DeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ResourceGroupTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewayVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListGateways"
```

```
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayGatewayStarPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackup*",
        "arn:aws:iam::*:role/*AWSBackup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "backup.amazonaws.com",
            "restore-testing.backup.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AwsOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:backup:backup-vault"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "backup.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemManagerCommandPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SystemManagerSendCommandPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:DescribeBackups",
        "fsx:DescribeVolumes",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DeleteBackup",
      "Resource" : "arn:aws:fsx:*:*:backup/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DirectoryServicePermissions",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "IamCreateServiceLinkedRolePermissions",
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "backup.amazonaws.com",
            "restore-testing.backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BackupGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:AssociateGatewayToServer",
        "backup-gateway:CreateGateway",
        "backup-gateway:DeleteGateway",
        "backup-gateway:DeleteHypervisor",
        "backup-gateway:DisassociateGatewayFromServer",
        "backup-gateway:ImportHypervisorConfiguration",
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup-gateway:PutMaintenanceStartTime",
        "backup-gateway:TagResource",
        "backup-gateway:TestHypervisorConfiguration",
        "backup-gateway:UntagResource",
        "backup-gateway:UpdateGatewayInformation",
        "backup-gateway:UpdateHypervisor"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayHypervisorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings",
        "backup-gateway:PutHypervisorPropertyMappings",
        "backup-gateway:StartVirtualMachinesMetadataSync"
      ],
```

```
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "BackupGatewayVirtualMachinePermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetVirtualMachine"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "BackupGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway",
        "backup-gateway:PutBandwidthRateLimitSchedule"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
    },
    {
      "Sid" : "CloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListTables",
        "timestream:ListDatabases"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "RedshiftResourcesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeSnapshotSchedules"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:subnetgroup:*",
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:snapshotschedule:*"
      ]
    },
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeNodeConfigurationOptions",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterTracks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListWorkgroups"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessDeletetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudFormationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
```

```
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "SystemsManagerForSapPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceAccessManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
```

```
      "Sid" : "IamPassRolePermissionsForGuardDuty",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackupGuardDuty*",
        "arn:aws:iam::*:role/*AWSBackupGuardDuty*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Descrição: Fornece AWS BackupGateway permissão para sincronizar os metadados das máquinas virtuais em seu nome

`AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço

- Hora da criação: 15 de dezembro de 2022, 19:43 UTC
- Hora da edição: 15 de dezembro de 2022, 19:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListVmTags",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "VMTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:TagResource",
        "backup-gateway:UntagResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupGuardDutyRolePolicyForScans

Descrição: Fornece GuardDuty permissão para ler seus pontos de recuperação AWS de backup para escaneamentos de malware

`AWSBackupGuardDutyRolePolicyForScans` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBackupGuardDutyRolePolicyForScans` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 20 de novembro de 2025, 03:34 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupGuardDutyRolePolicyForScans`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:ListChangedBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "StringLike" : {
          "aws:ResourceTag/aws:backup:source-resource" : "*"
        }
      }
    },
    {
      "Sid" : "CreateGrantForEncryptedVolumeCreation",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:guardduty:id" : "snap-*",
          "kms:ViaService" : [
            "guardduty.*.amazonaws.com",
            "backup.*.amazonaws.com"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "CreateGrant",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
          ]
        },
```

```
        "Null" : {
          "kms:GrantOperations" : "false"
        }
      }
    },
    {
      "Sid" : "CreateGrantForReEncryptAndEBSDirect",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "snap-*",
          "kms:ViaService" : [
            "guardduty.*.amazonaws.com",
            "backup.*.amazonaws.com"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
          ]
        },
        "Null" : {
          "kms:GrantOperations" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeKeyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "EC2ReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ShareSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "StringLike" : {
          "aws:ResourceTag/aws:backup:source-resource" : "*"
        }
      }
    },
    {
      "Sid" : "ShareSnapshotKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : [
            "vol-*",
            "snap-*"
          ],
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateBackupAccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupAccessPoint"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*"
```

```
    },
    {
      "Sid" : "ReadAndDeleteBackupAccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeBackupAccessPoint",
        "backup:DeleteBackupAccessPoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupRecoveryPointApiPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeRecoveryPoint"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*"
    },
    {
      "Sid" : "DecryptKMSEncryptedDataByAWSBackup",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:backup:backup-vault" : "*",
          "kms:ViaService" : "backup.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupOperatorAccess

Descrição: Essa política concede aos usuários permissões para atribuir AWS recursos a planos de backup, criar backups sob demanda e restaurar backups. Essa política não permite que o usuário crie ou edite planos de backup ou exclua backups agendados após sua criação.

`AWSBackupOperatorAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBackupOperatorAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de novembro de 2019, 22:23 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOperatorAccess`

Versão da política

Versão da política: v28 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
        "backup:CreateBackupSelection",
```

```
        "backup:DeleteBackupSelection",
        "backup:StartBackupJob",
        "backup:StartRestoreJob",
        "backup:StartCopyJob",
        "backup:StartScanJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBAccess",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSAccess",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
```

```
    },
    {
      "Sid" : "EC2Access",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:describeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewaySCSIAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayReadAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "storagegateway:ListGateways"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "StorageGatewayDiskReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayVolumeReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackup*",
        "arn:aws:iam::*:role/*AWSBackup*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMComandAccess",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FSXDescribeAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FSxFileAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FSxVolumeAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*/*"
    },
    {
      "Sid" : "FSxMachineAccess",
```

```
      "Effect" : "Allow",
      "Action" : "fsx:DescribeStorageVirtualMachines",
      "Resource" : "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
    },
    {
      "Sid" : "DirectoryServiceAccess",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayListAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayHypervisorAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "BackupGatewayMachineAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetVirtualMachine"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "BackupGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway"
```

```
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
    },
    {
      "Sid" : "CloudWatchAccess",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamListAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ListAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "RedshiftAccess",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeSnapshotSchedules"
```

```
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:subnetgroup:*",
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:snapshotschedule:*"
      ]
    },
    {
      "Sid" : "RedshiftOptionsAccess",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeNodeConfigurationOptions",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterTracks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
```

```
    },
    {
      "Sid" : "CloudFormationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "SAPAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SAPDatabaseAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    },
    {
      "Sid" : "RAMAccess",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "IamPassRolePermissionsForGuardDuty",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackupGuardDuty*",
        "arn:aws:iam::*:role/*AWSBackupGuardDuty*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupOrganizationAdminAccess

Descrição: política destinada a administradores de backup que usam o gerenciamento de backup entre contas para gerenciar backups para a organização.

`AWSBackupOrganizationAdminAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBackupOrganizationAdminAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de junho de 2020, 16:23 UTC
- Hora da edição: 18 de novembro de 2022, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DisableAWSServiceAccess",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:account/*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:AttachPolicy",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:DetachPolicy",
        "organizations:DisablePolicyType",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListPolicies",
        "organizations:EnablePolicyType",
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:PolicyType" : [
            "BACKUP_POLICY"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupRestoreAccessForSAPHANA

Descrição: Fornece permissão de AWS backup para restaurar um backup do SAP HANA no Amazon EC2

`AWSBackupRestoreAccessForSAPHANA` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBackupRestoreAccessForSAPHANA` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 10 de novembro de 2022, 22:43 UTC
- Hora da edição: 10 de novembro de 2022, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
        "backup:StartBackupJob",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:RestoreDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupSearchOperatorAccess

Descrição: a função do operador de pesquisa tem acesso para a criação de índices de backup e pesquisas nos metadados de backup indexados. Essa política contém as permissões necessárias para essas funções do operador de pesquisa.

`AWSBackupSearchOperatorAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBackupSearchOperatorAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 27 de fevereiro de 2025, 21:52 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC

- ARN: `arn:aws:iam::aws:policy/AWSBackupSearchOperatorAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartSearchAndListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-search:StartSearchJob",
        "backup-search:ListSearchJobs",
        "backup-search:ListSearchResultExportJobs",
        "backup:ListIndexedRecoveryPointsForSearch"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupSearchRecoveryPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:SearchRecoveryPoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:backup:*:*:recovery-point:*"
      ]
    },
    {
      "Sid" : "SearchAndExportPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-search:StartSearchResultExportJob",
```

```
        "backup-search:StopSearchJob",
        "backup-search:GetSearchJob",
        "backup-search:GetSearchResultExportJob",
        "backup-search:ListSearchJobResults",
        "backup-search:ListSearchJobBackups"
      ],
      "Resource" : [
        "arn:aws:backup-search:*:*:search-job/*",
        "arn:aws:backup-search:*:*:search-export-job/*"
      ]
    },
    {
      "Sid" : "KMSDataKeyForSearchAndExportPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:backup-search:search-job"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : [
            "backup.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupServiceLinkedRolePolicyForBackup

Descrição: Fornece permissão de AWS backup para criar backups em seu nome em todos AWS os serviços

`AWSBackupServiceLinkedRolePolicyForBackup` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 02 de junho de 2020, 23:08 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

Versão da política

Versão da política: v31 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EFSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
```

```
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    },
    {
      "Sid" : "DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "elasticfilesystem:DescribeFileSystems",
        "dynamodb:ListTables",
        "storagegateway:ListVolumes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstances",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnapshotCopyTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Sid" : "EC2CreateBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
```

```
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AWSBackupManagedResource"
          ]
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2RDSDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeImages",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBClusterSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
```

```
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CopyImage",
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "RDSInstanceAndSnashotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBSnapshot",
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBInstanceAutomatedBackup"
      ],
      "Resource" : "arn:aws:rds:*:*:snapshot:awsbackup:*"
    },
    {
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBClusterSnapshot",
        "rds:DeleteDBClusterSnapshot"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
    },
    {
      "Sid" : "RDSSnapshotTenantDatabasePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "rds:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:snapshot-tenant-database:awsbackup:*"
      ]
    },
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
```

```
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CopyBackup",
        "fsx:TagResource",
        "fsx:DescribeBackups",
        "fsx:DeleteBackup"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "DynamoDBDeletePermissions",
      "Effect" : "Allow",
      "Action" : "dynamodb:DeleteBackup",
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "BackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListTagsForBackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTagsOfResource",
```

```
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "EventBridgePermissions",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Sid" : "EventBridgeRulesPermissions",
      "Effect" : "Allow",
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:UpdateHANABackupSettings"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeTable",
        "timestream:GetAwsBackupStatus",
        "timestream:GetAwsRestoreStatus"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
```

```
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessDeleteSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudformationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "DSQLListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "OrgsListDelegatedAdmins",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EKSClusterConfigurationBackup",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster",
        "eks:ListAddons",
        "eks:DescribeAddon",
        "eks:ListNodegroups",
        "eks:DescribeNodegroup",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListFargateProfiles",
        "eks:DescribeFargateProfile",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupServiceLinkedRolePolicyForBackupTest

Descrição: Fornece permissão de AWS backup para criar backups em seu nome em todos AWS os serviços

`AWSBackupServiceLinkedRolePolicyForBackupTest` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 12 de maio de 2020, 17:37 UTC
- Hora da edição: 12 de maio de 2020, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
```

```
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Effect" : "Allow",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    },
    {
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupServiceRolePolicyForBackup

Descrição: Fornece permissão de AWS backup para criar backups em seu nome em todos AWS os serviços

`AWSBackupServiceRolePolicyForBackup` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBackupServiceRolePolicyForBackup` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 10 de janeiro de 2019, 21:01 UTC
- Horário editado: 23 de fevereiro de 2026, 19:42 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup`

Versão da política

Versão da política: v30 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:CreateBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeBackup",
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "DynamoDBBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:ListTagsForResource",
        "rds:DescribeDBSnapshots",
        "rds:CreateDBSnapshot",
```

```
        "rds:CopyDBSnapshot",
        "rds:DescribeDBInstances",
        "rds:CreateDBClusterSnapshot",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:CopyDBClusterSnapshot",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSInstanceAutomatedBackupPermissions",
      "Effect" : "Allow",
      "Action" : "rds:DeleteDBInstanceAutomatedBackup",
      "Resource" : "arn:aws:rds:*:*:auto-backup:*"
    },
    {
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBCluster"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RDSClusterBackupPermissions",
      "Effect" : "Allow",
      "Action" : "rds:DeleteDBClusterAutomatedBackup",
      "Resource" : "arn:aws:rds:*:*:cluster-auto-backup:*"
    },
    {
      "Sid" : "RDSModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
    },
    {
      "Sid" : "RDSBackupPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBSnapshot",
        "rds:ModifyDBSnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "RDSClusterModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBClusterSnapshot",
        "rds:ModifyDBClusterSnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:CreateSnapshot",
        "storagegateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "EBSTagAndDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSnapshotTierStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:image/*"
    },
    {
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:ModifyImageAttribute"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "EBSSnapshotTierPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "BackupVaultPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeBackupVault",
        "backup:CopyIntoBackupVault"
      ],
      "Resource" : "arn:aws:backup:*:*:backup-vault:*"
    },
    {
      "Sid" : "BackupVaultCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:CopyFromBackupVault"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
```

```
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "EBSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSDynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "KMSEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:ebs:id"
        }
      }
    },
    {
      "Sid" : "GetResourcesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSendPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxCreateBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:CreateBackup",
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
    {
      "Sid" : "FsxListTagsPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:ListTagsForResource",
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
```

```
      "Action" : "fsx:DeleteBackup",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:CopyBackup",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "DynamodbBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:StartAwsBackupJob",
        "dynamodb:ListTagsOfResource"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "BackupGatewayBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:Backup",
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "CloudformationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*/*"
    },
    {
```

```
      "Sid" : "RedshiftCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateClusterSnapshot",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessCreatePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*",
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
```

```
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:StartAwsBackupJob",
        "timestream:GetAwsBackupStatus",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListTagsForResource",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "DSQLResourcePermissionsForBackup",
      "Effect" : "Allow",
      "Action" : [
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSDSQLPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
        }
      }
    },
    {
      "Sid" : "EKSClusterConfigurationBackup",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster",
        "eks:ListAddons",
        "eks:DescribeAddon",
        "eks:ListNodegroups",
        "eks:DescribeNodegroup",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListFargateProfiles",
        "eks:DescribeFargateProfile",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateBackupAccessEntry",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateAccessEntry"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
```

```
    },
    {
      "Sid" : "AssociateBackupAccessPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
        "StringEquals" : {
          "eks:policyArn" : "arn:aws:eks::aws:cluster-access-policy/
AWSBackupFullAccessPolicyForBackup",
          "eks:accessScope" : "cluster"
        }
      }
    },
    {
      "Sid" : "GuardDutyMalwareScanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:StartMalwareScan",
        "guardduty:GetMalwareScan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyMalwareScanIAMPassPermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupServiceRolePolicyForIndexing

Descrição: Política contendo as permissões necessárias para que o AWS Backup indexe pontos de recuperação.

`AWSBackupServiceRolePolicyForIndexing` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBackupServiceRolePolicyForIndexing` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 17 de dezembro de 2024, 18:37 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForIndexing`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnlyPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "KMSDataKeyForEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupServiceRolePolicyForItemRestores

Descrição: Política contendo as permissões necessárias para que o AWS Backup restaure itens individuais em um ponto de recuperação

`AWSBackupServiceRolePolicyForItemRestores` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBackupServiceRolePolicyForItemRestores` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 17 de dezembro de 2024, 18:37 UTC
- Horário editado: 12 de fevereiro de 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForItemRestores`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnlyPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "S3ReadonlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3PermissionsForFileLevelRestore",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::*/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSDataKeyForS3AndEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "s3.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupServiceRolePolicyForRestores

Descrição: Fornece permissão AWS de backup para realizar restaurações em seu nome em todos AWS os serviços. Essa política inclui permissões para criar e excluir AWS recursos, como volumes do EBS, instâncias do RDS e sistemas de arquivos EFS, que fazem parte do processo de restauração.

`AWSBackupServiceRolePolicyForRestores` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBackupServiceRolePolicyForRestores` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 12 de janeiro de 2019, 0:23 UTC
- Horário editado: 27 de agosto de 2026, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

Versão da política

Versão da política: v36 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:PutItem",
        "dynamodb:GetItem",
        "dynamodb:DeleteItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
```

```
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "EBSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "EC2DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTagsPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonFSx" : "ManagedByAmazonFSx"
        }
      }
    },
    {
      "Sid" : "StorageGatewayVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DeleteVolume",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes",
        "storagegateway:AddTagsToResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:CreateStorediSCSIVolume",
        "storagegateway:CreateCachediSCSIVolume"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "RDSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
```

```
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:RestoreDBInstanceFromDBSnapshot",
        "rds:DeleteDBInstance",
        "rds:AddTagsToResource",
        "rds:DescribeDBClusters",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:DeleteDBCluster",
        "rds:RestoreDBInstanceToPointInTime",
        "rds:DescribeDBClusterSnapshots",
        "rds:RestoreDBClusterToPointInTime",
        "rds:CreateTenantDatabase",
        "rds:DeleteTenantDatabase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Restore",
        "elasticfilesystem:CreateFilesystem",
        "elasticfilesystem:DescribeFilesystems",
        "elasticfilesystem:DeleteFilesystem",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLResourcePermissionsForRestore",
      "Effect" : "Allow",
      "Action" : [
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:TagResource",
        "dsql:CreateCluster",
        "dsql:PutMultiRegionProperties",
```

```
        "dsql:PutWitnessRegion",
        "dsql:UpdateCluster",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetCluster"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com",
            "ec2.*.amazonaws.com",
            "elasticfilesystem.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "dsql.*.amazonaws.com",
            "redshift-serverless.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
```

```
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "EBSSnapshotBlockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:CompleteSnapshot",
        "ebs:StartSnapshot",
        "ebs:PutSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "RDSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBInstance"
      ],
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Sid" : "EC2DeleteAndRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:RestoreSnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsScopedPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
```

```
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:backup:source-resource"
          ]
        }
      }
    },
    {
      "Sid" : "EC2RunInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TerminateInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateVolume"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateFileSystemFromBackup"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*"
      ]
    },
    {
      "Sid" : "FsxTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteFileSystem",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "FsxDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "fsx:DescribeVolumes"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
    {
      "Sid" : "FsxVolumeTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:backup:source-resource"
          ]
        }
      }
    },
    {
      "Sid" : "FsxBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:storage-virtual-machine/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteVolume",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "DSPermissions",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromAwsBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "GatewayRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:Restore"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "CloudformationChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:*/*/*"
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:RestoreFromClusterSnapshot",
        "redshift:RestoreTableFromClusterSnapshot"
```

```
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftTablePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeTableRestoreStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:RestoreTableFromSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessNamespacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace"
      ],
      "Resource" : [
```

```
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessTablePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetTableRestoreStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:StartAwsRestoreJob",
        "timestream:GetAwsRestoreStatus",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:ListDatabases",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EKSClusterRestore",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateCluster",
```

```
        "eks:DescribeCluster",
        "eks:CreateAccessEntry",
        "eks:DescribeAccessEntry",
        "eks:AssociateAccessPolicy",
        "eks:ListAssociatedAccessPolicies",
        "eks:CreateAddon",
        "eks:DescribeAddon",
        "eks:CreateNodegroup",
        "eks:DescribeNodegroup",
        "eks:CreateFargateProfile",
        "eks:DescribeFargateProfile",
        "eks:CreatePodIdentityAssociation",
        "eks:DescribePodIdentityAssociation",
        "eks:TagResource"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:access-entry/*",
        "arn:aws:eks:*:*:addon/*",
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:eks:*:*:fargateprofile/*",
        "arn:aws:eks:*:*:nodegroup/*",
        "arn:aws:eks:*:*:podidentityassociation/*"
      ]
    },
    {
      "Sid" : "AssociateRestoreAccessPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
        "StringEquals" : {
          "eks:accessScope" : "cluster",
          "eks:policyArn" : "arn:aws:eks::aws:cluster-access-policy/
AWSBackupFullAccessPolicyForRestore"
        }
      }
    },
    {
      "Sid" : "CreateClusterIAMPerms",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "eks.amazonaws.com",
            "ec2.amazonaws.com",
            "pods.eks.amazonaws.com",
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEKSNodeGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSubnets",
        "ec2:RunInstances",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSNodeGroupTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "BackupRestoreJobManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:StartRestoreJob",
        "backup:ListRestoreJobs",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:DescribeRestoreJob"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupServiceRolePolicyForS3Backup

Descrição: Política contendo as permissões necessárias para que o AWS Backup faça backup de dados em qualquer bucket do S3. Isso inclui acesso de leitura a todos os objetos do S3 e qualquer acesso de descriptografia para todas as chaves do KMS.

`AWSBackupServiceRolePolicyForS3Backup` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBackupServiceRolePolicyForS3Backup` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de fevereiro de 2022, 17:40 UTC

- Horário editado: 24 de agosto de 2026, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchGetMetricDataPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridgePermissionsForAwsBackupManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Sid" : "EventBridgeListRulesPermissions",
      "Effect" : "Allow",
```

```
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketTagging",
        "s3:GetInventoryConfiguration",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:GetBucketAcl",
        "s3:PutInventoryConfiguration",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "S3ObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectAcl",
        "s3:GetObject",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion"
```

```
      ],
      "Resource" : "arn:aws:s3:::*/*"
    },
    {
      "Sid" : "S3ListBucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListAllMyBuckets",
      "Resource" : "*"
    },
    {
      "Sid" : "S3BucketTagReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListTagsForResource"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupServiceRolePolicyForS3Restore

Descrição: Política contendo as permissões necessárias para que o AWS Backup restaure um backup do S3 em um bucket. Isso inclui read/write permissões para todos os buckets do S3 e permissões para GenerateDataKey e DescribeKey para todas as chaves KMS.

`AWSBackupServiceRolePolicyForS3Restore` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBackupServiceRolePolicyForS3Restore` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de fevereiro de 2022, 17:39 UTC
- Hora da edição: 07 de fevereiro de 2023, 0:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:PutBucketVersioning",
        "s3:PutBucketOwnershipControls",
        "s3:GetBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:DeleteObject",
        "s3:PutObjectVersionAcl",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging",
        "s3:GetObjectAcl",
        "s3:PutObjectAcl",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBackupServiceRolePolicyForScans

Descrição: Fornece permissão AWS de backup para realizar verificações de malware em seus pontos de recuperação AWS de backup

`AWSBackupServiceRolePolicyForScans` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBackupServiceRolePolicyForScans` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 20 de novembro de 2025, 03:34 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForScans`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyMalwareScanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:StartMalwareScan",
        "guardduty:GetMalwareScan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassPermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBatchFullAccess

Descrição: fornece acesso total aos recursos do AWS Batch.

`AWSBatchFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBatchFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de dezembro de 2016, 19:35 UTC
- Hora da edição: 24 de outubro de 2022, 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBatchFullAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "batch:*",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ecs:DescribeClusters",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeCluster",
        "eks:ListClusters",
        "logs:Describe*",
        "logs:Get*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSBatchServiceRole",
        "arn:aws:iam::*:role/service-role/AWSBatchServiceRole",
        "arn:aws:iam::*:role/ecsInstanceRole",
        "arn:aws:iam::*:instance-profile/ecsInstanceRole",
        "arn:aws:iam::*:role/iaws-ec2-spot-fleet-role",
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-role",
        "arn:aws:iam::*:role/AWSBatchJobRole*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/*Batch*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "batch.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBatchServiceEventTargetRole

Descrição: Política para habilitar o CloudWatch Event Target para envio AWS de trabalhos em lote

`AWSBatchServiceEventTargetRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBatchServiceEventTargetRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 28 de fevereiro de 2018, 22:31 UTC
- Hora da edição: 28 de fevereiro de 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "batch:SubmitJob"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBatchServiceRole

Descrição: Política para a função de serviço AWS Batch que permite acesso a serviços relacionados, incluindo EC2, Autoscaling, EC2 Container Service e Cloudwatch Logs.

`AWSBatchServiceRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBatchServiceRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 06 de dezembro de 2016, 19:36 UTC
- Horário editado: 25 de agosto de 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole`

Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBatchPolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeLaunchTemplateVersions",
```

```
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:TerminateInstances",
        "ec2:RunInstances",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:SuspendProcesses",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:ListAccountSettings",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:RegisterTaskDefinition",
        "ecs:DeregisterTaskDefinition",
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:UpdateCluster",
        "ecs:UpdateContainerAgent",
        "ecs:DeregisterContainerInstance",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
```

```
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "iam:GetInstanceProfile",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement2",
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : [
        "arn:aws:ecs:*:*:task/*_Batch_*"
      ]
    },
    {
      "Sid" : "AWSBatchPolicyStatement3",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement4",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "autoscaling.amazonaws.com",
            "ecs.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement5",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBatchServiceRolePolicyForSageMaker

Descrição: Fornece acesso ao AWS Batch para colocar em fila e gerenciar cargas de trabalho da Amazon SageMaker

`AWSBatchServiceRolePolicyForSageMaker` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 15 de julho de 2025, 21:37 UTC
- Horário editado: 16 de abril de 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBatchServiceRolePolicyForSageMaker`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:ListTags",
        "sagemaker:DeleteTrainingJob"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:training-job/AWSBatch*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:CreateTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:training-job/AWSBatch*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateTrainingJob"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTrainingJobs",
        "sagemaker:Search"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBCMDataExportsServiceRolePolicy

Descrição: Uma função vinculada ao serviço para fornecer às exportações de dados de gerenciamento de custos e cobrança acesso aos dados do AWS serviço para exportar os dados para um local de destino, como o Amazon S3, em nome de um cliente.

`AWSBCMDataExportsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 10 de junho de 2024, 17:40 UTC
- Hora da edição: 10 de junho de 2024, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBCMDataExportsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationRecommendationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy

Descrição: permite que o Bedrock AgentCore Gateway gerencie os recursos do VPC Lattice em seu nome

`AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Horário de criação: 28 de março de 2026, 22:12 UTC
- Horário editado: 28 de março de 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBedrockAgentCoreGatewayNetworkServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSLRActionsForLattice",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowResourceGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:CreateResourceGateway",
        "vpc-lattice:TagResource"
      ],
```

```
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:resourcegateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/BedrockAgentCoreGatewayManaged" : "true",
          "aws:ResourceTag/BedrockAgentCoreGatewayManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowEC2PermissionsForResourceGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowResourceGatewayDelete",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeleteResourceGateway",
        "vpc-lattice:GetResourceGateway"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/BedrockAgentCoreGatewayManaged" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy

Descrição: permite que a Bedrock AgentCore Identity gerencie os recursos do VPC Lattice em seu nome

`AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 15 de abril de 2026, 00:42 UTC
- Horário editado: 15 de abril de 2026, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBedrockAgentCoreIdentityNetworkServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSLRActionsForLattice",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowResourceGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:CreateResourceGateway",
        "vpc-lattice:TagResource"
      ],
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:resourcegateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/BedrockAgentCoreIdentityManaged" : "true",
          "aws:ResourceTag/BedrockAgentCoreIdentityManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowEC2PermissionsForResourceGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowResourceGatewayDelete",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeleteResourceGateway",
        "vpc-lattice:GetResourceGateway"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/BedrockAgentCoreIdentityManaged" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBedrockAgentCoreRuntimeInstancesServiceRolePolicy

Descrição: permite que as instâncias do Bedrock AgentCore Runtime gerenciem recursos de computação em seu nome.

`AWSBedrockAgentCoreRuntimeInstancesServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Tempo de criação: 05 de agosto de 2026, 09:57 UTC
- Horário editado: 05 de agosto de 2026, 09:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBedrockAgentCoreRuntimeInstancesServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribeResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "AllowCleanupManagedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCleanupAutoScalingGroup",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:CompleteLifecycleAction"
      ],
      "Resource" : "arn:aws:autoscaling:*:*:autoScalingGroup:*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/bedrock-agentcore:capacity-provider-id" : "false"
        }
      }
    },
    {
      "Sid" : "AllowCleanupEventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "bedrock-agentcore.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AllowCleanupEBSVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowDetachEBSVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowTerminateManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "bedrock-agentcore.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBillingConductorFullAccess

Descrição: use a política AWSBillingConductorFullAccess gerenciada para permitir acesso completo ao console AWS Billing Conductor (ABC) e às APIs. Essa política permite que os usuários listem, criem e excluam recursos ABC.

`AWSBillingConductorFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBillingConductorFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 13 de abril de 2022, 18:02 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorFullAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:*",
        "organizations:ListAccounts",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:DescribeResponsibilityTransfer",
        "organizations:ListInboundResponsibilityTransfers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBillingConductorReadOnlyAccess

Descrição: use a política AWSBillingConductorReadOnlyAccess gerenciada para permitir acesso somente para leitura ao console AWS Billing Conductor (ABC) e às APIs. Essa política concede permissão para obter e listar todos os recursos do IAM. A política não inclui a capacidade de criar ou excluir recursos.

`AWSBillingConductorReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBillingConductorReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 13 de abril de 2022, 18:02 UTC
- Horário editado: 21 de setembro de 2026, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:List*",
        "billingconductor:GetBillingGroupCostReport",
        "billingconductor:GetBillingTransferPreference",
        "organizations:ListAccounts",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
```

```
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:DescribeResponsibilityTransfer",
        "organizations:ListInboundResponsibilityTransfers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBillingConductorRolePolicy

Descrição: Fornece AWS Billing Conductor acesso para gerenciar grupos de cobrança e recursos relacionados

`AWSBillingConductorRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 21 de setembro de 2026, 19:07 UTC
- Horário editado: 21 de setembro de 2026, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBillingConductorRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "billingconductor:CreateBillingGroup",
      "Resource" : [
        "arn:aws:billingconductor::*:billinggroup/*",
        "arn:aws:billingconductor::*:pricingplan/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "billingconductor:GetBillingTransferPreference",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeResponsibilityTransfer",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBillingReadOnlyAccess

Descrição: permite que os usuários visualizem as faturas no Console de Faturamento.

`AWSBillingReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBillingReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de agosto de 2020, 20:08 UTC
- Horário editado: 30 de julho de 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess`

Versão da política

Versão da política: v28 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:ViewBilling",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
```

```
        "billing:GetCredits",
        "billing:GetContractInformation",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "budgets:ViewBudget",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostCategoryDefinitions",
        "ce:ListCostCategoryResourceAssociations",
        "ce:ListTagsForResource",
        "ce:ListCostAllocationTags",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:GetTags",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsageComparisons",
        "ce:GetCostComparisonDrivers",
        "consolidatedbilling:ListLinkedAccounts",
        "consolidatedbilling:GetAccountBillingRole",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:DescribeReportDefinitions",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:GetAccountPlanState",
        "freetier:GetAccountActivity",
        "freetier:ListAccountActivities",
        "invoicing:BatchGetInvoiceProfile",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:GetInvoiceUnit",
        "invoicing:GetInvoiceCorrection",
        "invoicing:ListInvoiceSummaries",
        "invoicing:ListInvoiceUnits",
        "invoicing:GetProcurementPortalPreference",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:ListTagsForResource",
        "invoicing:ListInvoiceCorrections",
        "invoicing:ListProcurementPortals",
```

```
        "invoicing:ListProcurementPortalSuppliers",
        "mapcredits:ListQuarterSpend",
        "mapcredits:ListAssociatedPrograms",
        "mapcredits:ListQuarterCredits",
        "payments:GetFinancingApplication",
        "payments:GetFinancingLine",
        "payments:GetFinancingLineWithdrawal",
        "payments:GetFinancingOption",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListFinancingApplications",
        "payments:ListFinancingLines",
        "payments:ListFinancingLineWithdrawals",
        "payments:ListPaymentInstruments",
        "payments:ListPaymentPreferences",
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "sustainability:GetCarbonFootprintSummary",
        "tax:GetTaxRegistrationDocument",
        "tax:GetTaxInheritance",
        "tax:ListTaxRegistrations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBillingServiceRolePolicy

Descrição: permite que o serviço de cobrança valide o acesso aos dados para a visualização das cobranças derivadas.

`AWSBillingServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 11 de setembro de 2025, 16:19 UTC
- Horário editado: 11 de setembro de 2025, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBillingServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billing:GetBillingViewData"
```

```
      ],
      "Resource" : "arn:aws:billing::*:billingview/*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

Descrição: Essa política concede permissões para controlar AWS recursos. Por exemplo, para iniciar e interromper instâncias do EC2 ou do RDS executando scripts do AWS Systems Manager (SSM).

`AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de maio de 2022, 19:03 UTC
- Horário editado: 07 de abril de 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "rds:DescribeDBInstances",
        "rds:StartDBInstance",
        "rds:StopDBInstance"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-StartEC2Instance",
        "arn:aws:ssm:*:*:document/AWS-StopEC2Instance",
        "arn:aws:ssm:*:*:document/AWS-StartRdsInstance",
        "arn:aws:ssm:*:*:document/AWS-StopRdsInstance",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartRdsInstance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopRdsInstance:*"
```

```
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBudgetsActionsWithAWSResourceControlAccess

Descrição: Fornece acesso total às ações de AWS orçamentos, incluindo o uso de ações de orçamentos para controlar os estados dos recursos em execução por meio de AWS Console de gerenciamento da AWS

`AWSBudgetsActionsWithAWSResourceControlAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBudgetsActionsWithAWSResourceControlAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de outubro de 2020, 17:19 UTC
- Hora da edição: 15 de outubro de 2020, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "budgets:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "budgets.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ModifyBilling",
        "ec2:DescribeInstances",
        "iam:ListGroups",
        "iam:ListPolicies",
        "iam:ListRoles",
```

```
        "iam:ListUsers",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListPolicies",
        "organizations:ListRoots",
        "rds:DescribeDBInstances",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBudgetsReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao AWS Budgets Console por meio do. Console de gerenciamento da AWS

`AWSBudgetsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBudgetsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de outubro de 2020, 17:18 UTC
- Hora da edição: 17 de junho de 2024, 17:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBudgetsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*",
        "budgets:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBudgetsSpendLimitMemberRolePolicy

Descrição: Concede ao serviço de AWS orçamentos permissões para descrever, interromper e encerrar recursos em uma conta membro para impor ações de limite de gastos.

`AWSBudgetsSpendLimitMemberRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 18 de julho de 2026, 00:57 UTC
- Horário editado: 13 de agosto de 2026, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBudgetsSpendLimitMemberRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:StopInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeAddresses",
        "ec2:DescribeSnapshots",
        "ec2:DescribeInstanceStatus",
```

```
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSActions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:StopDBInstance",
        "rds:DescribeDBClusters",
        "rds:StopDBCluster",
        "rds:CreateDBClusterSnapshot",
        "rds:DescribeDBClusterSnapshots",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:DescribeIntegrations",
        "rds:DescribeDBProxies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLActions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:ListNotebookInstances",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StartNotebookInstance",
        "sagemaker:DescribeApp",
        "sagemaker:ListApps",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:ListTrainingJobs",
        "sagemaker:StopTrainingJob",
        "sagemaker:DescribeProcessingJob",
```

```
        "sagemaker:ListProcessingJobs",
        "sagemaker:StopProcessingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:StopTransformJob",
        "sagemaker:ListEndpoints",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:DescribeCluster",
        "sagemaker:ListClusters",
        "sagemaker:DescribeClusterNode",
        "sagemaker:ListClusterNodes",
        "sagemaker:AttachClusterNodeVolume",
        "sagemaker:DetachClusterNodeVolume",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:StopLabelingJob",
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaActions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:GetFunctionConcurrency",
        "lambda:PutFunctionConcurrency",
        "lambda:DeleteFunctionConcurrency",
        "lambda:ListEventSourceMappings",
        "lambda:GetEventSourceMapping",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:DeleteProvisionedConcurrencyConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:ListProvisionedModelThroughputs",
        "bedrock:UpdateProvisionedModelThroughput",
        "bedrock:GetModelInvocationJob",
        "bedrock:ListModelInvocationJobs",
        "bedrock:StopModelInvocationJob",
        "bedrock:GetModelCustomizationJob",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:StopModelCustomizationJob",
        "bedrock:GetEvaluationJob",
        "bedrock:ListEvaluationJobs",
        "bedrock:StopEvaluationJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:GetAutomationExecution",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-StartEC2Instance",
        "arn:aws:ssm:*:*:document/AWS-StopEC2Instance",
        "arn:aws:ssm:*:*:document/AWS-StartRdsInstance",
        "arn:aws:ssm:*:*:document/AWS-StopRdsInstance",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartRdsInstance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopRdsInstance:*"
      ]
    },
    {
      "Sid" : "CostOptimizationHubActions",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:UpdateEnrollmentStatus",
        "cost-optimization-hub:ListEnrollmentStatuses"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeOptimizerActions",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:GetIdleRecommendations",
        "compute-optimizer:GetRecommendationSummaries",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:UpdateEnrollmentStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeOptimizerAutomationActions",
      "Effect" : "Allow",
      "Action" : [
        "aco-automation:StartAutomationEvent",
        "aco-automation:ListRecommendedActions",
        "aco-automation:GetAutomationEvent",
        "aco-automation:GetEnrollmentConfiguration",
        "aco-automation:UpdateEnrollmentConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOActions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccountActions",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetPrimaryEmail"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowAWSServiceAccessForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "arn:aws:organizations:*:*:*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com",
            "compute-optimizer.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowACOAutomationSLRCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/aco-automation.amazonaws.com/
AWSServiceRoleForComputeOptimizerAutomation",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "aco-automation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowComputeOptimizerSLRCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/cost-optimization-hub.bcm.amazonaws.com/
AWSServiceRoleForCostOptimizationHub",
        "arn:aws:iam::*:role/aws-service-role/compute-optimizer.amazonaws.com/
AWSServiceRoleForComputeOptimizer",
        "arn:aws:iam::*:role/aws-service-role/aco-automation.amazonaws.com/
AWSServiceRoleForComputeOptimizerAutomation"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "compute-optimizer.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "AllowCostOptimizationHubSLRCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cost-optimization-
hub.bcm.amazonaws.com/AWSServiceRoleForCostOptimizationHub",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cost-optimization-hub.bcm.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBugBustFullAccess

Descrição: essa política do IAM concede aos usuários acesso total ao AWS BugBust console

`AWSBugBustFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBugBustFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de junho de 2021, 7:03 UTC
- Hora da edição: 22 de julho de 2021, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeGuruProfilerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-profiler:DescribeProfilingGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "bugbust:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustSLRCreation",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/bugbust.amazonaws.com/
AWSServiceRoleForBugBust",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "bugbust.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBugBustPlayerAccess

Descrição: essa política do IAM concede aos usuários acesso para participar de AWS BugBust eventos

`AWSBugBustPlayerAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSBugBustPlayerAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de junho de 2021, 7:15 UTC
- Hora da edição: 24 de junho de 2021, 7:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustPlayerAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeGuruProfilerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:DescribeProfilingGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustPlayerAccess",
      "Effect" : "Allow",
      "Action" : [
        "bugbust:ListBugs",
        "bugbust:ListProfilingGroups",
        "bugbust:JoinEvent",
        "bugbust:GetEvent",
        "bugbust:ListEvents",
        "bugbust:GetJoinEventStatus",
        "bugbust:ListEventScores",
        "bugbust:ListEventParticipants",
        "bugbust:UpdateWorkItem",
```

```
        "bugbust:ListPullRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSBugBustServiceRolePolicy

Descrição: Concede permissões AWS BugBust para acessar recursos em seu nome

`AWSBugBustServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 24 de junho de 2021, 6:59 UTC
- Hora da edição: 24 de junho de 2021, 6:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCertificateManagerFullAccess

Descrição: Fornece acesso total ao AWS Certificate Manager (ACM)

`AWSCertificateManagerFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCertificateManagerFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 21 de janeiro de 2016, 17:02 UTC
- Hora da edição: 17 de agosto de 2020, 22:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "acm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCertificateManagerPrivateCAAuditor

Descrição: Fornece acesso do auditor à Autoridade de AWS Certificação Privada do Certificate Manager

`AWSCertificateManagerPrivateCAAuditor` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCertificateManagerPrivateCAAuditor` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de outubro de 2018, 16:51 UTC
- Hora da edição: 17 de agosto de 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:CreateCertificateAuthorityAuditReport",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:GetPolicy",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCertificateManagerPrivateCAFullAccess

Descrição: Fornece acesso total à Autoridade de AWS Certificação Privada do Certificate Manager

`AWSCertificateManagerPrivateCAFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCertificateManagerPrivateCAFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de outubro de 2018, 16:54 UTC
- Hora da edição: 23 de outubro de 2018, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "acm-pca:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCertificateManagerPrivateCAPrivilegedUser

Descrição: Fornece acesso privilegiado ao usuário do certificado à Autoridade de AWS Certificação Privada do Certificate Manager

`AWSCertificateManagerPrivateCAPrivilegedUser` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCertificateManagerPrivateCAPrivilegedUser` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 20 de junho de 2019, 17:43 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
```

```
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCertificateManagerPrivateCAReadOnly

Descrição: Fornece acesso somente para leitura à Autoridade de AWS Certificação Privada do Certificate Manager

`AWSCertificateManagerPrivateCAReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCertificateManagerPrivateCAReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de outubro de 2018, 16:57 UTC
- Hora da edição: 17 de agosto de 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:ListCertificateAuthorities",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:GetPolicy",
      "acm-pca:ListPermissions",
      "acm-pca:ListTags"
    ],
    "Resource" : "*"
  }
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCertificateManagerPrivateCAUser

Descrição: Fornece ao usuário do certificado acesso à Autoridade de AWS Certificação Privada do Certificate Manager

`AWSCertificateManagerPrivateCAUser` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCertificateManagerPrivateCAUser` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de outubro de 2018, 16:53 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
```

```
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCertificateManagerReadOnly

Descrição: Fornece acesso somente para leitura ao AWS Certificate Manager (ACM).

`AWSCertificateManagerReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCertificateManagerReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 21 de janeiro de 2016, 17:07 UTC
- Horário editado: 13 de agosto de 2026, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:SearchCertificates",
      "acm:GetCertificate",
```

```
      "acm:ListTagsForCertificate",
      "acm:GetAccountConfiguration",
      "acm:DescribeAcmeAccount",
      "acm:DescribeAcmeDomainValidation",
      "acm:DescribeAcmeEndpoint",
      "acm:DescribeAcmeExternalAccountBinding",
      "acm:ListAcmeAccounts",
      "acm:ListAcmeDomainValidations",
      "acm:ListAcmeEndpoints",
      "acm:ListAcmeExternalAccountBindings",
      "acm:ListTagsForResource",
      "acm:ListCertificateDomainValidations"
    ],
    "Resource" : "*"
  }
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSChatbotServiceLinkedRolePolicy

Descrição: A função vinculada ao serviço usada pelo AWS Chatbot.

`AWSChatbotServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 18 de novembro de 2019, 16:39 UTC

- Hora da edição: 18 de novembro de 2019, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Unsubscribe",
        "sns:Subscribe",
        "sns:ListSubscriptions"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/chatbot/*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCleanRoomsFullAccess

Descrição: Permite acesso total aos recursos do AWS Clean Rooms e acesso aos relacionados Serviços da AWS.

`AWSCleanRoomsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCleanRoomsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 12 de janeiro de 2023, 16:10 UTC
- Hora da edição: 21 de março de 2024, 15:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickQueryResultsBucketListAll",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SetQueryResultsBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
    },
    {
```

```
      "Sid" : "WriteQueryResults",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleDisplayQueryResults",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
    },
    {
      "Sid" : "EstablishLogDeliveries",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCleanRoomsFullAccessNoQuerying

Descrição: Permite acesso total aos recursos do AWS Clean Rooms, exceto para consultas em uma colaboração e acesso a recursos relacionados Serviços da AWS.

`AWSCleanRoomsFullAccessNoQuerying` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCleanRoomsFullAccessNoQuerying` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 12 de janeiro de 2023, 16:12 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:CreateAnalysisTemplate",
        "cleanrooms:CreateCollaboration",
        "cleanrooms:CreateConfiguredTable",
        "cleanrooms:CreateConfiguredTableAnalysisRule",
        "cleanrooms:CreateConfiguredTableAssociation",
        "cleanrooms:CreateMembership",
        "cleanrooms:DeleteAnalysisTemplate",
        "cleanrooms:DeleteCollaboration",
        "cleanrooms:DeleteConfiguredTable",
        "cleanrooms:DeleteConfiguredTableAnalysisRule",
        "cleanrooms:DeleteConfiguredTableAssociation",
        "cleanrooms:DeleteMember",
        "cleanrooms:DeleteMembership",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
```

```
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:UpdateAnalysisTemplate",
        "cleanrooms:UpdateCollaboration",
        "cleanrooms:UpdateConfiguredTable",
        "cleanrooms:UpdateConfiguredTableReference",
        "cleanrooms:UpdateConfiguredTableAllowedColumns",
        "cleanrooms:UpdateConfiguredTableAnalysisRule",
        "cleanrooms:UpdateConfiguredTableAssociation",
        "cleanrooms:UpdateMembership",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:UntagResource",
        "cleanrooms:TagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CleanRoomsNoQuerying",
      "Effect" : "Deny",
      "Action" : [
        "cleanrooms:StartProtectedQuery",
        "cleanrooms:UpdateProtectedQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
```

```
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EstablishLogDeliveries",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCleanRoomsMLFullAccess

Descrição: Permite acesso total aos recursos de ML do AWS Clean Rooms e acesso aos relacionados Serviços da AWS.

`AWSCleanRoomsMLFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCleanRoomsMLFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2023, 21:02 UTC
- Horário editado: 12 de fevereiro de 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsMLFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cleanrooms-ml*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms-ml.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CollaborationMembershipCheck",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:ListMembers"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cleanrooms-ml.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AssociateModels",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:CreateConfiguredAudienceModelAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagAssociations",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:TagResource"
      ],
      "Resource" : "arn:aws:cleanrooms:*:*:membership/*/
configuredaudiencemodelassociation/*"
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/cleanrooms-ml*",
        "arn:aws:iam::*:role/role/cleanrooms-ml*"
      ]
```

```
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanroomsml*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickOutputBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickS3Location",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*cleanrooms-ml*"
    },
    {
      "Sid" : "ConsoleDescribeECRRepositories",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeRepositories",
        "ecr:ListImages"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*"
    },
    {
      "Sid" : "PassCleanRoomsResources",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:PassMembership",
        "cleanrooms:PassCollaboration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCleanRoomsMLReadOnlyAccess

Descrição: Permite acesso somente para leitura aos recursos de ML do AWS Clean Rooms e acesso somente para leitura aos recursos relacionados ao Clean Rooms AWS

`AWSCleanRoomsMLReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCleanRoomsMLReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2023 de 20:55 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
```

```
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CleanRoomsMLRead",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:Get*",
        "cleanrooms-ml:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassCleanRoomsResources",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:PassMembership",
        "cleanrooms:PassCollaboration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCleanRoomsReadOnlyAccess

Descrição: Permite acesso somente para leitura aos recursos do AWS Clean Rooms e acesso somente para leitura aos recursos relacionados do AWS Glue e do Amazon Logs. CloudWatch

`AWSCleanRoomsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCleanRoomsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 12 de janeiro de 2023, 16:10 UTC
- Hora da edição: 12 de janeiro de 2023, 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsRead",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGet*",
        "cleanrooms:Get*",
        "cleanrooms:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCleanRoomsServiceRolePolicy

Descrição: Permita que o AWS Clean Rooms acesse outros AWS serviços, como CloudWatch APIs, em seu nome.

`AWSCleanRoomsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 15 de dezembro de 2025, 17:49 UTC
- Horário editado: 15 de dezembro de 2025, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCleanRoomsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Clean Rooms"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloud9Administrator

Descrição: Fornece acesso de administrador ao AWS Cloud9.

`AWSCloud9Administrator` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCloud9Administrator` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de novembro de 2017, 16:17 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:*",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
```

```
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloud9EnvironmentMember

Descrição: Fornece a capacidade de ser convidado para ambientes de desenvolvimento compartilhados do AWS Cloud9.

`AWSCloud9EnvironmentMember` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCloud9EnvironmentMember` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de novembro de 2017, 16:18 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:GetUserSettings",
        "cloud9:UpdateUserSettings",
        "cloud9:GetMigrationExperiences",
        "iam:GetUser",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloud9:DescribeEnvironmentMemberships"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true",
          "cloud9:EnvironmentId" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
```

```
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloud9ServiceRolePolicy

Descrição: Política de função vinculada ao serviço para AWS Cloud9

`AWSCloud9ServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 30 de novembro de 2017, 13:44 UTC
- Horário editado: 03 de setembro de 2026, 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "ec2:TerminateInstances",
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-cloud9-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
```

```
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : "aws-cloud9-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "aws-cloud9-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : [
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/cloud9/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSCloud9SSMAccessRole"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloud9SSMInstanceProfile

Descrição: essa política será usada para anexar uma função em uma InstanceProfile que permitirá que o Cloud9 use o SSM Session Manager para se conectar à instância.

`AWSCloud9SSMInstanceProfile` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCloud9SSMInstanceProfile` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de maio de 2020, 11:40 UTC
- Hora da edição: 14 de maio de 2020, 11:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloud9User

Descrição: Fornece permissão para criar ambientes de desenvolvimento do AWS Cloud9 e gerenciar ambientes próprios.

`AWSCloud9User` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCloud9User` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de novembro de 2017, 16:16 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9User`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:UpdateUserSettings",
        "cloud9:GetUserSettings",
        "cloud9:GetMigrationExperiences",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:CreateEnvironmentEC2",
        "cloud9:CreateEnvironmentSSH"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "cloud9:OwnerArn" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:GetUserPublicKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloud9:DescribeEnvironmentMemberships"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true",
          "cloud9:EnvironmentId" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
```

```
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloudFormationFullAccess

Descrição: Fornece acesso total AWS CloudFormation a.

`AWSCloudFormationFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCloudFormationFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de julho de 2019, 21:50 UTC
- Hora da edição: 26 de julho de 2019, 21:50 UTC

- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloudFormationReadOnlyAccess

Descrição: Fornece AWS CloudFormation acesso ao Console de gerenciamento da AWS.

`AWSCloudFormationReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCloudFormationReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:39 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:BatchDescribe*",
        "cloudformation:EstimateTemplateCost",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudformation:Detect*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloudFrontLogger

Descrição: Concede ao CloudFront Logger permissões de gravação nos CloudWatch registros.

`AWSCloudFrontLogger` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 12 de junho de 2018, 20:15 UTC
- Hora da edição: 22 de novembro de 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloudFrontVPCOriginServiceRolePolicy

Descrição: Permite CloudFront gerenciar interfaces de rede elástica e grupos de segurança do EC2 em seu nome.

`AWSCloudFrontVPCOriginServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 24 de outubro de 2024, 17:45 UTC
- Hora da edição: 24 de outubro de 2024, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontVPCOriginServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Action1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "EC2Action2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "EC2Action3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "EC2Action4",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "EC2Action5",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action7",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled",
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "CreateSecurityGroup"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "ElbAction1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloudHSMFullAccess

Descrição: fornece acesso total a todos os recursos do CloudHSM.

`AWSCloudHSMFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCloudHSMFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:39 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudhsm:*",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloudHSMReadOnlyAccess

Descrição: fornece acesso somente leitura a todos os recursos do CloudHSM.

`AWSCloudHSMReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCloudHSMReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:39 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:Get*",
        "cloudhsm:List*",
        "cloudhsm:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloudHSMRole

Descrição: Política padrão para a função de serviço do AWS CloudHSM.

`AWSCloudHSMRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCloudHSMRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloudMapDiscoverInstanceAccess

Descrição: Fornece acesso à API de descoberta de Nuvem AWS mapas.

`AWSCloudMapDiscoverInstanceAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCloudMapDiscoverInstanceAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2018, 0:02 UTC
- Hora da edição: 20 de setembro de 2023, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloudMapFullAccess

Descrição: Fornece acesso total a todas as ações do Nuvem AWS mapa.

`AWSCloudMapFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCloudMapFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2018, 23:57 UTC
- Hora da edição: 29 de julho de 2020, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "servicediscovery:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloudMapReadOnlyAccess

Descrição: Fornece acesso somente para leitura a todas as ações do Nuvem AWS Mapa.

`AWSCloudMapReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCloudMapReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2018, 23:45 UTC
- Hora da edição: 20 de setembro de 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloudMapRegisterInstanceAccess

Descrição: Fornece acesso em nível de registrante às ações do Nuvem AWS Mapa.

`AWSCloudMapRegisterInstanceAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCloudMapRegisterInstanceAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2018, 0:04 UTC
- Hora da edição: 20 de setembro de 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
```

```
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloudShellFullAccess

Descrição: Concede uso AWS CloudShell com todos os recursos

`AWSCloudShellFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCloudShellFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 15 de dezembro de 2020, 18:07 UTC
- Hora da edição: 15 de dezembro de 2020, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudshell:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloudTrail_FullAccess

Descrição: Fornece acesso total AWS CloudTrail a.

`AWSCloudTrail_FullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCloudTrail_FullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de outubro de 2020, 23:41 UTC
- Hora da edição: 22 de fevereiro de 2021, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns:GetTopicAttributes"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudtrail:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRolePolicy",
```

```
        "iam:GetUser"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateKey",
        "kms:CreateAlias",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloudTrail_ReadOnlyAccess

Descrição: Fornece acesso somente para AWS CloudTrail leitura a.

`AWSCloudTrail_ReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCloudTrail_ReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de junho de 2022, 17:19 UTC
- Hora da edição: 14 de junho de 2022, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:Get*",
        "cloudtrail:Describe*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

Descrição: Essa política é usada pela função vinculada ao serviço chamada AWSServiceRoleForCloudWatchAlarms _ActionSSMIncidents. CloudWatch usa essa função vinculada ao serviço para realizar ações AWS do System Manager Incident Manager quando um CloudWatch alarme entra no estado ALARM. Esta política concede permissão para iniciar incidentes em seu nome.

`AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Hora da criação: 27 de abril de 2021, 13:30 UTC
- Hora da edição: 27 de abril de 2021, 13:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCloudWatchOmniServiceRolePolicy

Descrição: fornece acesso CloudWatch Omni para gerenciar recursos do gravador de AWS configuração, configurações de telemetria e funções de suporte do IAM para capacitar a organização.

`AWSCloudWatchOmniServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 22 de setembro de 2026, 05:37 UTC
- Horário editado: 24 de setembro de 2026, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchOmniServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateManagedCloudWatchIntegration",
      "Effect" : "Allow",
      "Action" : "cloudwatch:CreateIntegration",
      "Resource" : "arn:aws:cloudwatch:*:*:integration/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOmniManaged"
        },
        "StringEquals" : {
          "aws:RequestTag/CloudWatchOmniManaged" : "true",
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagOperationForCloudWatchIntegration",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:integration/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOmniManaged"
        },
        "StringEquals" : {
          "aws:RequestTag/CloudWatchOmniManaged" : "true",
          "aws:ResourceTag/CloudWatchOmniManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListCloudWatchIntegration",
      "Effect" : "Allow",
      "Action" : "cloudwatch:ListIntegrations",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeleteManagedCloudWatchIntegration",
      "Effect" : "Allow",
      "Action" : "cloudwatch:DeleteIntegration",
      "Resource" : "arn:aws:cloudwatch:*:*:integration/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchOmniManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "ManageConfigServiceLinkedRecorder",
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorderStatus",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Resource" : "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForCloudWatch/*"
    },
    {
      "Sid" : "CreateConfigServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateCloudWatchOmniAWSIntegrationRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/CloudWatchOmniAWSIntegrationRole-
*",
      "Condition" : {
        "ArnEquals" : {
          "iam:RoleTemplateARN" : "arn:aws:iam::aws:role-template/
cloudwatch.amazonaws.com/CloudWatchOmniAWSIntegrationForOrgRoleTemplate:1"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "ReadRoleTemplate",
      "Effect" : "Allow",
      "Action" : "iam:GetRoleTemplateVersion",
      "Resource" : "arn:aws:iam::aws:role-template/cloudwatch.amazonaws.com/
CloudWatchOmniAWSIntegrationForOrgRoleTemplate:1"
    },
    {
      "Sid" : "PassRolePermissionForCloudWatchOmniAWSIntegrationRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/CloudWatchOmniAWSIntegrationRole-
*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cloudwatch.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListIamUsersAndRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetAwsAccountInformation",
      "Effect" : "Allow",
      "Action" : "account:GetAccountInformation",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "GetCloudWatchOmniAWSIntegrationRole",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/service-role/CloudWatchOmniAWSIntegrationRole-
*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeArtifactAdminAccess

Descrição: Fornece acesso AWS CodeArtifact total ao Console de gerenciamento da AWS.

`AWSCodeArtifactAdminAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeArtifactAdminAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 16 de junho de 2020, 23:53 UTC
- Hora da edição: 16 de junho de 2020, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeArtifactReadOnlyAccess

Descrição: Fornece acesso somente para leitura AWS CodeArtifact por meio do Console de gerenciamento da AWS.

`AWSCodeArtifactReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeArtifactReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de junho de 2020, 21:23 UTC
- Hora da edição: 25 de junho de 2020, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:Describe*",
        "codeartifact:Get*",
        "codeartifact:List*",
        "codeartifact:ReadFromRepository"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeBuildAdminAccess

Descrição: Fornece acesso AWS CodeBuild total ao Console de gerenciamento da AWS. Anexe também AmazonS3ReadOnlyAccess para fornecer acesso ao download de artefatos de construção e anexe IAMFullAccess para criar e gerenciar a função de serviço para CodeBuild.

`AWSCodeBuildAdminAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeBuildAdminAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2016, 19:04 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess`

Versão da política

Versão da política: v20 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "codecommit:ListRepositories",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "elasticfilesystem:DescribeFileSystems",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CWLDeleteLogGroupAccess",
      "Action" : [
        "logs:DeleteLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*:log-stream:*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
    },
    {
      "Sid" : "SSMStartSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "SSMOpenDataChannelAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Sid" : "CodeStarConnectionsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:CreateConnection",
        "codestar-connections:DeleteConnection",
        "codestar-connections:UpdateConnectionInstallation",
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar-connections:ListConnections",
```

```
        "codestar-connections:ListInstallationTargets",
        "codestar-connections:ListTagsForResource",
        "codestar-connections:GetConnection",
        "codestar-connections:GetIndividualAccessToken",
        "codestar-connections:GetInstallationUrl",
        "codestar-connections:PassConnection",
        "codestar-connections:StartOAuthHandshake",
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeBuildDeveloperAccess

Descrição: Fornece acesso AWS CodeBuild por meio do Console de gerenciamento da AWS, mas não permite a administração CodeBuild do projeto. Anexe também AmazonS3ReadOnlyAccess para fornecer acesso ao download de artefatos de construção.

`AWSCodeBuildDeveloperAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeBuildDeveloperAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2016, 19:02 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess`

Versão da política

Versão da política: v21 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:StartBuildBatch",
        "codebuild:StopBuildBatch",
        "codebuild:RetryBuild",
        "codebuild:RetryBuildBatch",
```

```
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codebuild:List*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
    },
    {
      "Sid" : "SSMStartSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "SSMOpenDataChannelAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
```

```
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeBuildReadOnlyAccess

Descrição: Fornece acesso somente para leitura AWS CodeBuild por meio do Console de gerenciamento da AWS. Anexe também AmazonS3ReadOnlyAccess para fornecer acesso ao download de artefatos de construção.

`AWSCodeBuildReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeBuildReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2016, 19:03 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess`

Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:List*",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeCommitFullAccess

Descrição: Fornece acesso AWS CodeCommit total ao Console de gerenciamento da AWS.

`AWSCodeCommitFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeCommitFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de julho de 2015, 17:02 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

Versão da política

Versão da política: v13 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:*"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
```

```
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codecommit:*:*:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:AssociateRepository",
        "codeguru-reviewer:DescribeRepositoryAssociation",
```

```
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DisassociateRepository",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeCommitPowerUser

Descrição: Fornece acesso total aos AWS CodeCommit repositórios, mas não permite a exclusão do repositório.

`AWSCodeCommitPowerUser` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeCommitPowerUser` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de julho de 2015, 17:06 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitPowerUser`

Versão da política

Versão da política: v18 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:AssociateApprovalRuleTemplateWithRepository",
        "codecommit:BatchAssociateApprovalRuleTemplateWithRepositories",
        "codecommit:BatchDisassociateApprovalRuleTemplateFromRepositories",
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Create*",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:Describe*",
        "codecommit:DisassociateApprovalRuleTemplateFromRepository",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:Merge*",
        "codecommit:OverridePullRequestApprovalRules",
        "codecommit:Put*",
        "codecommit:Post*",
        "codecommit:TagResource",
        "codecommit:Test*",
        "codecommit:UntagResource",
        "codecommit:Update*",
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
```

```
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codecommit:*:*:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:AssociateRepository",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DisassociateRepository",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
```

```
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeCommitReadOnly

Descrição: Fornece acesso somente para leitura AWS CodeCommit por meio do Console de gerenciamento da AWS.

`AWSCodeCommitReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeCommitReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de julho de 2015, 17:05 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Describe*",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:GitPull"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials",
        "iam:ListAccessKeys",
        "iam:GetSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codecommit:*:*:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
```

```
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeDeployDeployerAccess

Descrição: fornece acesso para registrar e implantar uma revisão.

`AWSCodeDeployDeployerAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeDeployDeployerAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 19 de maio de 2015, 18:18 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:CreateDeployment",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codedeploy:RegisterApplicationRevision"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
```

```
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codedeploy:*:*:application:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeDeployFullAccess

Descrição: Fornece acesso total aos CodeDeploy recursos.

`AWSCodeDeployFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeDeployFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 19 de maio de 2015, 18:13 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "codedeploy:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
```

```
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codedeploy:*:*:application:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeDeployReadOnlyAccess

Descrição: Fornece acesso somente para leitura aos CodeDeploy recursos.

`AWSCodeDeployReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeDeployReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 19 de maio de 2015, 18:21 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codedeploy:*:*:application:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeDeployRole

Descrição: Fornece acesso ao CodeDeploy serviço para expandir tags e interagir com o Auto Scaling em seu nome.

`AWSCodeDeployRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeDeployRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 04 de maio de 2015, 18:05 UTC
- Horário editado: 10 de setembro de 2026, 10:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:DeleteLifecycleHook",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:PutLifecycleHook",
        "autoscaling:RecordLifecycleActionHeartbeat",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:EnableMetricsCollection",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:SuspendProcesses",
        "autoscaling:ResumeProcesses",
        "autoscaling:AttachLoadBalancers",
        "autoscaling:AttachLoadBalancerTargetGroups",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutWarmPool",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DeleteAutoScalingGroup",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:TerminateInstances",
        "tag:GetResources",
        "sns:Publish",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth",
```

```
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeDeployRoleForCloudFormation

Descrição: fornece acesso ao CodeDeploy serviço para invocar a função Lambda em seu nome para realizar a blue/green implantação por meio dele. CloudFormation

`AWSCodeDeployRoleForCloudFormation` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeDeployRoleForCloudFormation` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 19 de maio de 2020, 17:12 UTC
- Hora da edição: 19 de maio de 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeDeployRoleForECS

Descrição: Fornece acesso amplo ao CodeDeploy serviço para realizar uma blue/green implantação do ECS em seu nome. Concede acesso total aos serviços de suporte, como acesso total para ler todos os objetos do S3, invocar todas as funções do Lambda, publicar em todos os tópicos do SNS na conta e atualizar todos os serviços do ECS.

`AWSCodeDeployRoleForECS` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeDeployRoleForECS` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de novembro de 2018, 20:40 UTC
- Hora da edição: 23 de setembro de 2019, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
        "ecs:UpdateServicePrimaryTaskSet",
        "ecs:DeleteTaskSet",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:ModifyRule",
        "lambda:InvokeFunction",
        "cloudwatch:DescribeAlarms",
        "sns:Publish",
        "s3:GetObject",
```

```
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeDeployRoleForECSLimited

Descrição: Fornece acesso limitado ao CodeDeploy serviço para realizar uma blue/green implantação do ECS em seu nome.

`AWSCodeDeployRoleForECSLimited` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeDeployRoleForECSLimited` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de novembro de 2018, 20:42 UTC
- Hora da edição: 23 de setembro de 2019, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
        "ecs:UpdateServicePrimaryTaskSet",
        "ecs:DeleteTaskSet",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:CodeDeployTopic_*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
```

```
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:ModifyRule"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsTaskExecutionRole",
        "arn:aws:iam::*:role/ECSTaskExecution*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com"
          ]
        }
```

```
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeDeployRoleForLambda

Descrição: Fornece acesso ao CodeDeploy serviço para realizar uma implantação do Lambda em seu nome.

`AWSCodeDeployRoleForLambda` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeDeployRoleForLambda` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 28 de novembro de 2017, 14:05 UTC
- Hora da edição: 03 de dezembro de 2019, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "lambda:UpdateAlias",
        "lambda:GetAlias",
        "lambda:GetProvisionedConcurrencyConfig",
        "sns:Publish"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeDeployRoleForLambdaLimited

Descrição: Fornece acesso limitado ao CodeDeploy serviço para realizar uma implantação do Lambda em seu nome.

`AWSCodeDeployRoleForLambdaLimited` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeDeployRoleForLambdaLimited` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 17 de agosto de 2020, 17:14 UTC
- Hora da edição: 17 de agosto de 2020, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "lambda:UpdateAlias",
        "lambda:GetAlias",
        "lambda:GetProvisionedConcurrencyConfig"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
```

```
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodePipeline_FullAccess

Descrição: Fornece acesso AWS CodePipeline total ao Console de gerenciamento da AWS.

`AWSCodePipeline_FullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodePipeline_FullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 03 de agosto de 2020, 22:38 UTC
- Hora da edição: 14 de março de 2024, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ListChangeSets",
        "cloudtrail:DescribeTrails",
        "codebuild:BatchGetProjects",
        "codebuild:CreateProject",
        "codebuild:ListCuratedEnvironmentImages",
        "codebuild:ListProjects",
        "codecommit:ListBranches",
        "codecommit:GetReferences",
        "codecommit:ListRepositories",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:ListClusters",
        "ecs:ListServices",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "iam:ListRoles",
        "iam:GetRole",
        "lambda:ListFunctions",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:DescribeRule",
        "opsworks:DescribeApps",
        "opsworks:DescribeLayers",
        "opsworks:DescribeStacks",
        "s3:ListAllMyBuckets",
        "sns:ListTopics",
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
```

```
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes",
        "states:ListStateMachines"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "CodePipelineAuthoringAccess"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketPolicy",
        "s3:GetBucketVersioning",
        "s3:GetObjectVersion",
        "s3:CreateBucket",
        "s3:PutBucketPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3::*:codepipeline-*",
      "Sid" : "CodePipelineArtifactsReadWriteAccess"
    },
    {
      "Action" : [
        "cloudtrail:PutEventSelectors",
        "cloudtrail:CreateTrail",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:StartLogging"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudtrail:*:*:trail/codepipeline-source-trail",
      "Sid" : "CodePipelineSourceTrailReadWriteAccess"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/cwe-role-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "events.amazonaws.com"
          ]
        }
      },
      "Sid" : "EventsIAMPassRole"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "codepipeline.amazonaws.com"
          ]
        }
      },
      "Sid" : "CodePipelineIAMPassRole"
    },
    {
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:DisableRule",
        "events:RemoveTargets"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:events:*:*:rule/codepipeline-*"
      ],
      "Sid" : "CodePipelineEventsReadWriteAccess"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
```

```
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodePipeline_ReadOnlyAccess

Descrição: Fornece acesso somente para leitura AWS CodePipeline por meio do Console de gerenciamento da AWS.

`AWSCodePipeline_ReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodePipeline_ReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 03 de agosto de 2020, 22:25 UTC
- Hora da edição: 03 de agosto de 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListActionExecutions",
        "codepipeline:ListActionTypes",
```

```
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "s3:ListAllMyBuckets",
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3::*:codepipeline-*"
    },
    {
      "Sid" : "CodeStarNotificationsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodePipelineApproverAccess

Descrição: fornece acesso para visualizar e aprovar alterações manuais em todos os pipelines

`AWSCodePipelineApproverAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodePipelineApproverAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de julho de 2016, 18:59 UTC
- Hora da edição: 02 de agosto de 2017, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodePipelineCustomActionAccess

Descrição: Fornece acesso a ações personalizadas para pesquisar detalhes de trabalhos (incluindo credenciais temporárias) e relatar atualizações de status. AWS CodePipeline

`AWSCodePipelineCustomActionAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodePipelineCustomActionAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de julho de 2015, 17:02 UTC
- Hora da edição: 09 de julho de 2015, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeStarFullAccess

Descrição: Fornece acesso AWS CodeStar total ao Console de gerenciamento da AWS.

`AWSCodeStarFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeStarFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 19 de abril de 2017, 16:23 UTC
- Hora da edição: 28 de março de 2023, 0:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeStarFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeStarEC2",
      "Effect" : "Allow",
      "Action" : [
        "codestar:*",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "cloud9:DescribeEnvironment*",
        "cloud9:ValidateEnvironmentName"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarCF",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:ListStacks*",
        "cloudformation:GetTemplateSummary"
```

```
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeStarNotificationsServiceRolePolicy

Descrição: permite que AWS CodeStar as notificações acessem o Amazon CloudWatch Events em seu nome

`AWSCodeStarNotificationsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 05 de novembro de 2019, 16:10 UTC
- Hora da edição: 19 de março de 2020, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DescribeRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/awscodestarnotifications-*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:CodeStarNotifications-*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommentsForComparedCommit",
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:UpdateSlackChannelConfiguration",
        "codecommit:GetDifferences",
        "codepipeline:ListActionExecutions"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
```

```
        "codecommit:GetFile"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/ExcludeFileContentFromNotifications" : "true"
        }
      },
      "Effect" : "Allow"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCodeStarServiceRole

Descrição: NÃO USE — Política de função de AWS CodeStar serviço que concede privilégios administrativos CodeStar para gerenciar o IAM e outros recursos de serviço em nome do cliente.

`AWSCodeStarServiceRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCodeStarServiceRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 19 de abril de 2017, 15:20 UTC
- Horário editado: 08 de setembro de 2026, 12:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProjectEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:RemoveTargets",
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/awscodestar-*"
      ]
    },
    {
      "Sid" : "ProjectStack",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*Stack*",
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:GetTemplate"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*",
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/aws-cloud9-*",
        "arn:aws:cloudformation:*:aws:transform/CodeStar*"
      ]
    },
    {
      "Sid" : "ProjectStackTemplate",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeChangeSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*",
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/aws-cloud9-*",
        "arn:aws:cloudformation:*:aws:transform/CodeStar*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack",
            "CreateChangeSet",
            "ExecuteChangeSet"
          ]
        }
      }
    },
    {
      "Sid" : "ProjectQuickstarts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::awscodestar-*/*"
      ]
    },
    {
      "Sid" : "ProjectS3Buckets",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:*"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-codestar-*",
        "arn:aws:s3:::elasticbeanstalk-*"
      ]
    },
    {
      "Sid" : "ProjectServices",
      "Effect" : "Allow",
      "Action" : [
        "codestar:*",
        "codecommit:*",
        "codepipeline:*",
        "codedeploy:*",
        "codebuild:*",
        "autoscaling:*",
        "cloudwatch:Put*",
        "ec2:*",
        "elasticbeanstalk:*",
        "elasticloadbalancing:*",
        "iam:ListRoles",
        "logs:*",
        "sns:*",
        "cloud9:CreateEnvironmentEC2",
        "cloud9:DeleteEnvironment",
        "cloud9:DescribeEnvironment*",
        "cloud9:ListEnvironments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ProjectWorkerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRole",
        "iam:PassRole",
        "iam:GetRolePolicy",
        "iam:PutRolePolicy",
```

```
        "iam:SetDefaultPolicyVersion",
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CodeStarWorker*",
        "arn:aws:iam::*:policy/CodeStarWorker*",
        "arn:aws:iam::*:instance-profile/awscodestar-*"
      ]
    },
    {
      "Sid" : "ProjectTeamMembers",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachUserPolicy",
        "iam:DetachUserPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyArn" : [
            "arn:aws:iam::*:policy/CodeStar_*"
          ]
        }
      }
    },
    {
      "Sid" : "ProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicyVersions",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:policy/CodeStar_*"
      ]
    },
    {
      "Sid" : "InspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-codestar-service-role",
        "arn:aws:iam::*:role/service-role/aws-codestar-service-role"
      ]
    },
    {
      "Sid" : "IAMLinkRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DescribeConfigRuleForARN",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ProjectCodeStarConnections",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codestar-connections:GetConnection"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ProjectCodeStarConnectionsPassConnections",
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCompromisedKeyQuarantine

Descrição: nega o acesso a determinadas ações, aplicadas pela AWS equipe no caso de as credenciais de um usuário do IAM terem sido comprometidas ou expostas publicamente. NÃO remova essa política. Em vez disso, siga as instruções especificadas no e-mail enviado a você sobre este evento.

`AWSCompromisedKeyQuarantine` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCompromisedKeyQuarantine` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 11 de agosto de 2020, 18:04 UTC
- Hora da edição: 11 de agosto de 2020, 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateUser",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
```

```
        "lambda:CreateFunction",
        "lightsail:Create*",
        "lightsail:Start*",
        "lightsail:Delete*",
        "lightsail:Update*",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:DownloadDefaultKeyPair"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCompromisedKeyQuarantineV2

Descrição: nega o acesso a determinadas ações, aplicadas pela AWS equipe no caso de as credenciais de um usuário do IAM terem sido comprometidas ou expostas publicamente. NÃO remova essa política. Em vez disso, siga as instruções especificadas no caso de suporte criado para você em relação a esse evento.

`AWSCompromisedKeyQuarantineV2` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCompromisedKeyQuarantineV2` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 21 de abril de 2021, 22:30 UTC

- Hora da edição: 2 de outubro de 2024, 16:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreatePolicyVersion",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PassRole",
        "iam:PutGroupPolicy",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:UpdateAccessKey",
```

```
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateLoginProfile",
        "iam:UpdateUser",
        "lambda:AddLayerVersionPermission",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetPolicy",
        "lambda:ListTags",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lightsail:Create*",
        "lightsail:Delete*",
        "lightsail:DownloadDefaultKeyPair",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:Start*",
        "lightsail:Update*",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketAcl",
        "s3:PutBucketOwnershipControls",
        "s3:DeleteBucketPolicy",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:ListAllMyBuckets",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:AcceptReservedInstancesExchangeQuote",
        "ec2:CreateReservedInstancesListing",
        "savingsplans:CreateSavingsPlan",
        "ecs:CreateService",
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition",
        "ecr:GetAuthorizationToken",
        "bedrock:CreateModelInvocationJob",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:CreateFoundationModelAgreement",
```

```
        "bedrock:PutFoundationModelEntitlement",
        "bedrock:InvokeModel",
        "s3:CreateBucket",
        "s3:PutBucketCors",
        "s3:GetObject",
        "s3:ListBucket",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateProcessingJob",
        "ses:GetSendQuota",
        "ses:ListIdentities",
        "sts:GetSessionToken",
        "sts:GetFederationToken",
        "amplify:CreateDeployment",
        "amplify:CreateBackendEnvironment",
        "codebuild:CreateProject",
        "glue:CreateJob",
        "iam:DeleteRole",
        "iam:DeleteAccessKey",
        "iam:ListUsers",
        "lambda:GetEventSourceMapping",
        "sns:GetSMSAttributes",
        "mediapackagev2:CreateChannel"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCompromisedKeyQuarantineV3

Descrição: nega acesso a determinadas ações, aplicadas AWS caso as credenciais de um usuário do IAM tenham sido comprometidas ou expostas publicamente. A política visa limitar danos que podem ser causados por atividades relacionadas a fraudes que levem a cobranças não autorizadas, mas sem afetar os recursos existentes. NÃO remova essa política. Em vez disso, siga as instruções especificadas no caso de suporte criado para você em relação a esse evento.

`AWSCompromisedKeyQuarantineV3` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCompromisedKeyQuarantineV3` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 21 de agosto de 2024, 17:36 UTC
- Horário editado: 16 de março de 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV3`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
```

```
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:AcceptReservedInstancesExchangeQuote",
        "ec2:CreateReservedInstancesListing",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreatePolicyVersion",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PassRole",
        "iam:PutGroupPolicy",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateLoginProfile",
        "iam:UpdateUser",
        "iam:DeleteRole",
        "iam:DeleteAccessKey",
        "iam:ListUsers",
        "lambda:AddLayerVersionPermission",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetPolicy",
        "lambda:ListTags",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lambda:GetEventSourceMapping",
        "lightsail:Create*",
        "lightsail:Delete*",
        "lightsail:DownloadDefaultKeyPair",
```

```
        "lightsail:GetInstanceAccessDetails",
        "lightsail:Start*",
        "lightsail:Update*",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "organizations:LeaveOrganization",
        "organizations:AcceptHandshake",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketAcl",
        "s3:PutBucketOwnershipControls",
        "s3:DeleteBucketPolicy",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:ListAllMyBuckets",
        "s3:CreateBucket",
        "s3:PutBucketCors",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutEncryptionConfiguration",
        "savingsplans:CreateSavingsPlan",
        "ecs:CreateService",
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition",
        "ecr:GetAuthorizationToken",
        "bedrock:CreateModelInvocationJob",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:CreateFoundationModelAgreement",
        "bedrock:PutFoundationModelEntitlement",
        "bedrock:InvokeModel",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateProcessingJob",
        "ses:GetSendQuota",
        "ses:ListIdentities",
        "sts:GetSessionToken",
        "sts:GetFederationToken",
        "amplify:CreateDeployment",
        "amplify:CreateBackendEnvironment",
        "codebuild:CreateProject",
        "glue:CreateJob",
```

```
        "sns:GetSMSAttributes",
        "mediapackagev2:CreateChannel",
        "logs:PutLogEvents",
        "kms:PutKeyPolicy",
        "kms:RetireGrant",
        "kms:RevokeGrant",
        "kms:ScheduleKeyDeletion",
        "kms:DeleteImportedKeyMaterial"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:ViaService" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSConfigMultiAccountSetupPolicy

Descrição: permite que o Config chame AWS serviços e implante recursos de configuração em toda a organização

`AWSConfigMultiAccountSetupPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 17 de junho de 2019, 18:03 UTC
- Hora da edição: 24 de fevereiro de 2023, 1:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-
multiaccountsetup.amazonaws.com/*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack",
        "config:DeleteConformancePack"
      ],
      "Resource" : "arn:aws:config:*:*:conformance-pack/aws-service-conformance-pack/
config-multiaccountsetup.amazonaws.com/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConformancePackStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
        }
      }
    },
    {
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSConfigRemediationServiceRolePolicy

Descrição: permite que o AWS Config corrija recursos não compatíveis em seu nome.

`AWSConfigRemediationServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Horário da criação: 18 de junho de 2019, 21:21 UTC
- Hora da edição: 18 de junho de 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      },
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSConfigRoleForOrganizations

Descrição: permite que o AWS Config chame APIs de organizações somente para leitura AWS

`AWSConfigRoleForOrganizations` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSConfigRoleForOrganizations` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 19 de março de 2018, 22:53 UTC
- Hora da edição: 24 de novembro de 2020, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSConfigRulesExecutionRole

Descrição: permite que uma função do AWS Lambda acesse a API AWS Config e os snapshots de configuração que o AWS Config entrega periodicamente ao Amazon S3. Esse acesso é exigido por funções que avaliam as alterações de configuração das regras de Config personalizadas.

`AWSConfigRulesExecutionRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSConfigRulesExecutionRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 25 de março de 2016, 17:59 UTC
- Hora da edição: 13 de maio de 2019, 21:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/AWSLogs/*/Config/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:Put*",
        "config:Get*",
        "config:List*",
        "config:Describe*",
        "config:BatchGet*",
        "config:Select*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSConfigServiceRolePolicy

Descrição: permite que o Config chame AWS serviços e colete configurações de recursos em seu nome.

`AWSConfigServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 30 de maio de 2018, 23:31 UTC
- Horário editado: 23 de setembro de 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

Versão da política

Versão da política: v96 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigServiceRolePolicyStatementID1",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
```

```
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "access-analyzer:ValidatePolicy",
        "account-access:GetEntitlement",
        "account-access:ListEntitlements",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListTagsForResource",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListForms",
        "amplifyuibuilder:ListThemes",
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
```

```
        "aoss:ListVpcEndpoints",
        "app-integrations:GetApplication",
        "app-integrations:GetDataIntegration",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListApplications",
        "app-integrations:ListDataIntegrations",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
        "app-integrations:ListTagsForResource",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExperimentDefinition",
        "appconfig:GetExtension",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExperimentDefinitions",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource",
        "applicationinsights:DescribeApplication",
        "applicationinsights:DescribeComponent",
        "applicationinsights:DescribeLogPattern",
        "applicationinsights:ListApplications",
```

```
        "applicationinsights:ListComponents",
        "applicationinsights:ListLogPatterns",
        "applicationinsights:ListLogPatternSets",
        "applicationinsights:ListTagsForResource",
        "appmesh:DescribeGatewayRoute",
        "appmesh:DescribeMesh",
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:DescribeAppBlockBuilders",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appstream:ListAssociatedFleets",
        "appstream:ListAssociatedStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApi",
        "appsync:GetApiAssociation",
        "appsync:GetApiCache",
        "appsync:GetChannelNamespace",
```

```
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetGraphqlApi",
        "appsync:GetResolver",
        "appsync:GetSourceApiAssociation",
        "appsync:ListApis",
        "appsync:ListChannelNamespaces",
        "appsync:ListDataSources",
        "appsync:ListDomainNames",
        "appsync:ListGraphqlApis",
        "appsync:ListResolvers",
        "appsync:ListSourceApiAssociations",
        "appsync:ListTagsForResource",
        "appsync:ListTypes",
        "apptest:GetTestCase",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeAnomalyDetector",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration",
        "aps:DescribeResourcePolicy",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeScraperLoggingConfiguration",
        "aps:DescribeWorkspace",
        "aps:DescribeWorkspaceConfiguration",
        "aps:ListAnomalyDetectors",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "arc-region-switch:GetPlan",
        "arc-region-switch:ListPlans",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListTagsForResource",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
```

```
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetControl",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessments",
        "auditmanager:ListControls",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "b2bi:GetCapability",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:GetTransformer",
        "b2bi:ListCapabilities",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "b2bi:ListTagsForResource",
        "b2bi:ListTransformers",
        "backup-gateway:GetHypervisor",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:GetTieringConfiguration",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
```

```
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListRestoreTestingPlans",
        "backup:ListRestoreTestingSelections",
        "backup:ListTags",
        "backup:ListTieringConfigurations",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeConsumableResource",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobQueues",
        "batch:DescribeQuotaShare",
        "batch:DescribeSchedulingPolicies",
        "batch:DescribeServiceEnvironments",
        "batch:ListConsumableResources",
        "batch:ListQuotaShares",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "bcm-dashboards:GetDashboard",
        "bcm-dashboards:ListDashboards",
        "bcm-dashboards:ListTagsForResource",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:ListExports",
        "bcm-data-exports:ListTagsForResource",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetBrowserProfile",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetConfigurationBundle",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPaymentConnector",
        "bedrock-agentcore:GetPaymentCredentialProvider",
        "bedrock-agentcore:GetPaymentManager",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetPolicyEngineSummary",
```

```
        "bedrock-agentcore:GetPolicyGeneration",
        "bedrock-agentcore:GetPolicyGenerationSummary",
        "bedrock-agentcore:GetPolicySummary",
        "bedrock-agentcore:GetResourcePolicy",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBrowserProfiles",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListConfigurationBundles",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:ListPaymentConnectors",
        "bedrock-agentcore:ListPaymentCredentialProviders",
        "bedrock-agentcore:ListPaymentManagers",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListPolicyEngineSummaries",
        "bedrock-agentcore:ListPolicyGenerations",
        "bedrock-agentcore:ListPolicyGenerationSummaries",
        "bedrock-agentcore:ListPolicySummaries",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAutomatedReasoningPolicy",
        "bedrock:GetBlueprint",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataSource",
        "bedrock:GetEvaluationJob",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
```

```
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPromptRouter",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAutomatedReasoningPolicies",
        "bedrock:ListBlueprints",
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListDataSources",
        "bedrock:ListEnforcedGuardrailsConfiguration",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListFlowVersions",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "billing:GetBillingView",
        "billing:ListBillingViews",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "braket:ListTagsForResource",
        "braket:SearchSpendingLimits",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cases:BatchGetCaseRule",
```

```
        "cases:BatchGetField",
        "cases:GetDomain",
        "cases:GetLayout",
        "cases:GetTemplate",
        "cases:ListCaseRules",
        "cases:ListDomains",
        "cases:ListFields",
        "cases:ListLayouts",
        "cases:ListTemplates",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "chime:DescribeAppInstance",
        "chime:DescribeAppInstanceBot",
        "chime:DescribeAppInstanceUser",
        "chime:DescribeChannelFlow",
        "chime:ListAppInstanceBots",
        "chime:ListAppInstances",
        "chime:ListChannelFlows",
        "chime:ListTagsForResource",
        "cleanrooms-ml:GetConfiguredModelAlgorithm",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListConfiguredModelAlgorithms",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
```

```
        "cleanrooms:ListTagsForResource",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribePublisher",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListChangeSets",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
        "cloudfront:DescribeFunction",
        "cloudfront:DescribeKeyValueStore",
        "cloudfront:GetAnycastIpList",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetConnectionGroup",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistributionTenant",
        "cloudfront:GetFunction",
        "cloudfront:GetKeyGroup",
        "cloudfront:GetMonitoringSubscription",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:GetVpcOrigin",
        "cloudfront:ListAnycastIpLists",
        "cloudfront:ListCachePolicies",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListConnectionGroups",
        "cloudfront:ListContinuousDeploymentPolicies",
```

```
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListFunctions",
        "cloudfront:ListKeyGroups",
        "cloudfront:ListKeyValueStores",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudfront:ListVpcOrigins",
        "cloudtrail:DescribeTrails",
        "cloudTrail:GetChannel",
        "cloudtrail:GetDashboard",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudTrail:ListChannels",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:DescribeInsightRules",
        "cloudwatch:GetAlarmMuteRule",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListAlarmMuteRules",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListManagedInsightRules",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackageGroup",
        "codeartifact:DescribeRepository",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
```

```
        "codeartifact:ListAllowedRepositoriesForGroup",
        "codeartifact:ListDomains",
        "codeartifact:ListPackageGroups",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetFleets",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListFleets",
        "codebuild:ListReportGroups",
        "codebuild:ListSourceCredentials",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codedeploy:GetDeploymentConfig",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "codepipeline:ListWebhooks",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:ListConnections",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListTagsForResource",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:AdminGetUser",
        "cognito-idp:AdminListGroupsForUser",
```

```
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeManagedLoginBranding",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeTerms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListTerms",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "comprehend:DescribeFlywheel",
        "comprehend:ListFlywheels",
        "comprehend:ListTagsForResource",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:ListCampaigns",
        "connect:DescribeAgentStatus",
        "connect:DescribeDataTable",
        "connect:DescribeEmailAddress",
        "connect:DescribeEvaluationForm",
        "connect:DescribeHoursOfOperation",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribeMetric",
        "connect:DescribeNotification",
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
```

```
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUser",
        "connect:DescribeUserHierarchyGroup",
        "connect:DescribeUserHierarchyStructure",
        "connect:DescribeView",
        "connect:DescribeWorkspace",
        "connect:GetTaskTemplate",
        "connect:ListAgentStatuses",
        "connect:ListApprovedOrigins",
        "connect:ListDataTables",
        "connect:ListEvaluationForms",
        "connect:ListEvaluationFormVersions",
        "connect:ListHoursOfOperationOverrides",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListMetrics",
        "connect:ListNotifications",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPredefinedAttributes",
        "connect:ListPrompts",
        "connect:ListQueueEmailAddresses",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileManualAssignmentQueues",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileAIAgents",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfileFlowModules",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListTrafficDistributionGroups",
        "connect:ListUserHierarchyGroups",
```

```
        "connect:ListUsers",
        "connect:ListViews",
        "connect:ListViewVersions",
        "connect:ListWorkspaceMedia",
        "connect:ListWorkspacePages",
        "connect:ListWorkspaces",
        "connect:SearchAvailablePhoneNumbers",
        "connect:SearchWorkspaceAssociations",
        "controltower:GetLandingZone",
        "controltower:ListLandingZones",
        "cur:DescribeReportDefinitions",
        "cur:ListTagsForResource",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationAzureBlob",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxOntap",
        "datasync:DescribeLocationFsxOpenZfs",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "datazone:GetDomain",
```

```
        "datazone:GetDomainUnit",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentProfile",
        "datazone:GetGroupProfile",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListDomains",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListSubscriptionTargets",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "deadline:GetBudget",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetJob",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetQueueLimitAssociation",
        "deadline:GetStorageProfile",
        "deadline:ListBudgets",
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListJobs",
        "deadline:ListLicenseEndpoints",
        "deadline:ListMonitors",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListQueueLimitAssociations",
        "deadline:ListQueues",
```

```
        "deadline:ListStorageProfiles",
        "deadline:ListTagsForResource",
        "deadline:SearchJobs",
        "detective:ListGraphs",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListNotificationChannels",
        "directconnect:DescribeConnections",
        "dms:DescribeCertificates",
        "dms:DescribeDataMigrations",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationConfigs",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListDataProviders",
        "dms:ListInstanceProfiles",
        "dms:ListMigrationProjects",
        "dms:ListTagsForResource",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dsql:GetCluster",
        "dsql:GetClusterPolicy",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
```

```
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeTransitGatewayMeteringPolicies",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetRouteServerAssociations",
        "ec2:GetRouteServerPropagations",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:DescribeRepositoryCreationTemplates",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
```

```
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeExpressGatewayService",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeCapability",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListCapabilities",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
```

```
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:DescribeCapacityReservation",
        "elasticloadbalancing:DescribeListenerAttributes",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "elemental-inference:GetFeed",
        "elemental-inference:ListFeeds",
        "elemental-inference:ListTagsForResource",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
```

```
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetIdNamespace",
        "entityresolution:GetMatchingWorkflow",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "entityresolution:ListIdNamespaces",
        "entityresolution:ListMatchingWorkflows",
        "entityresolution:ListSchemaMappings",
        "entityresolution:ListTagsForResource",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
```

```
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:ListExperimentTemplates",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:ListPolicies",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "forecast:ListTagsForResource",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeFileSystems",
        "fsx:DescribeS3AccessPointAttachments",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeContainerFleet",
```

```
        "gamelift:DescribeContainerGroupDefinition",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScalingPolicies",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListContainerFleets",
        "gamelift:ListContainerGroupDefinitions",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "gamelift:ValidateMatchmakingRuleSet",
        "gameliftstreams:GetApplication",
        "gameliftstreams:GetStreamGroup",
        "gameliftstreams:ListApplications",
        "gameliftstreams:ListStreamGroups",
        "gameliftstreams:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeKey",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListKeys",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
```

```
        "globalaccelerator:DescribeAcceleratorAttributes",
        "globalaccelerator:DescribeCrossAccountAttachment",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCrossAccountAttachments",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:DescribeIntegrations",
        "glue:GetBlueprint",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetRegistry",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetSession",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetWorkflow",
        "glue:ListBlueprints",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
```

```
        "glue:ListRegistries",
        "glue:ListSessions",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:GetDeployment",
        "greengrass:ListComponents",
        "greengrass:ListComponentVersions",
        "greengrass:ListDeployments",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatEntitySet",
        "guardduty:GetThreatIntelSet",
        "guardduty:GetTrustedEntitySet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatEntitySets",
```

```
        "guardduty:ListThreatIntelSets",
        "guardduty:ListTrustedEntitySets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:GetDataTransformationProfile",
        "healthlake:ListDataTransformationProfiles",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
        "iam:ListMFADeviceTags",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
```

```
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
        "imagebuilder:ListWorkflowBuildVersions",
        "imagebuilder:ListWorkflows",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetCodeSecurityScanConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListCodeSecurityScanConfigurations",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "inspector2:ListTagsForResource",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:ListTagsForResource",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
```

```
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCertificateProvider",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJob",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetCommand",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:GetV2LoggingOptions",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificateProviders",
        "iot:ListCertificates",
        "iot:ListCommands",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPackages",
        "iot:ListPackageVersions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
```

```
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetStateTemplate",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:ListCampaigns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigServiceRolePolicyStatementID2",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListStateTemplates",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeComputationModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeDataset",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListComputationModels",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
```

```
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListDevicesForWirelessDeviceImportTask",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStorageConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
```

```
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListTagsForResource",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra-ranking:DescribeRescoreExecutionPlan",
        "kendra-ranking:ListRescoreExecutionPlans",
        "kendra-ranking:ListTagsForResource",
        "kendra:DescribeIndex",
        "kendra:ListDataSources",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetResourcePolicy",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
```

```
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeLakeFormationIdentityCenterConfiguration",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionScalingConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListCapacityProviders",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctions",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "launchwizard:GetDeployment",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListTagsForResource",
```

```
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "license-manager:ListTagsForResource",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperations",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
```

```
        "logs:DescribeDeliveries",
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeDestinations",
        "logs:DescribeIndexPolicies",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetIntegration",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
```

```
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindingsFilters",
        "macie2:ListTagsForResource",
        "managedblockchain:GetAccessor",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListAccessors",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeGateway",
        "mediaconnect:GetRouterInput",
        "mediaconnect:GetRouterNetworkInterface",
        "mediaconnect:ListBridges",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGateways",
        "mediaconnect:ListRouterInputs",
        "mediaconnect:ListRouterNetworkInterfaces",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListTagsForResource",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeNode",
        "medialive:DescribeSdiSource",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:ListChannelPlacementGroups",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListMultiplexes",
        "medialive:ListMultiplexPrograms",
        "medialive:ListNodes",
        "medialive:ListSdiSources",
```

```
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:DescribeAsset",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediatailor:DescribeChannel",
        "mediatailor:DescribeLiveSource",
        "mediatailor:DescribeSourceLocation",
        "mediatailor:DescribeVodSource",
        "mediatailor:GetChannelPolicy",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "medical-imaging:GetDatastore",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListTagsForResource",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetEmailChannel",
```

```
        "mobiletargeting:GetEmailTemplate",
        "mobiletargeting:GetEventStream",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:GetSegment",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTagsForResource",
        "mobiletargeting:ListTemplates",
        "mpa:GetIdentitySource",
        "mpa:ListIdentitySources",
        "mpa:ListTagsForResource",
        "mq:DescribeBroker",
        "mq:DescribeConfiguration",
        "mq:ListBrokers",
        "mq:ListConfigurations",
        "mq:ListTags",
        "neptune-graph:GetGraphSnapshot",
        "neptune-graph:ListGraphSnapshots",
        "neptune-graph:ListTagsForResource",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetDirectConnectGatewayAttachment",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
```

```
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:ListTagsForResource",
        "notifications:GetEventRule",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications:ListOrganizationalUnits",
        "notifications:ListTagsForResource",
        "nova-act:GetWorkflowDefinition",
        "nova-act:ListWorkflowDefinitions",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListLinks",
        "oam:ListSinks",
        "oam:ListTagsForResource",
        "omics:GetAnnotationStore",
        "omics:GetConfiguration",
        "omics:GetReferenceStore",
        "omics:GetRun",
        "omics:GetRunCache",
        "omics:GetRunGroup",
        "omics:GetS3AccessPolicy",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:GetWorkflowVersion",
        "omics:ListAnnotationStores",
        "omics:ListConfigurations",
        "omics:ListReferenceStores",
        "omics:ListRunCaches",
        "omics:ListRunGroups",
        "omics:ListRuns",
        "omics:ListSequenceStores",
        "omics:ListTagsForResource",
        "omics:ListVariantStores",
        "omics:ListWorkflows",
        "omics:ListWorkflowVersions",
```

```
        "opsworks:DescribeInstances",
        "opsworks:DescribeLayers",
        "opsworks:DescribeTimeBasedAutoScaling",
        "opsworks:DescribeVolumes",
        "opsworks:ListTags",
        "organizations:DescribeAccount",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "osis:GetPipeline",
        "osis:GetResourcePolicy",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "outposts:GetSite",
        "outposts:ListSites",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
```

```
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListChallengeMetadata",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetPolicy",
```

```
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:ListApplications",
        "qbusiness:ListDataSources",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeCustomPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeOAuthClientApplication",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:DescribeTopic",
        "quicksight:DescribeVPCConnection",
        "quicksight:ListAnalyses",
        "quicksight:ListCustomPermissions",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListFolders",
        "quicksight:ListOAuthClientApplications",
        "quicksight:ListRefreshSchedules",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "quicksight:ListTopics",
        "quicksight:ListVPCConnections",
        "ram:GetPermission",
```

```
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterDbRevisions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
```

```
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeDataShares",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:DescribeCollection",
        "rekognition:DescribeProjects",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListCollections",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
```

```
        "resource-groups:ListGroups",
        "robomaker:DescribeRobotApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListRobotApplications",
        "robomaker:ListSimulationApplications",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
```

```
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListOutpostResolvers",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver:ListTagsForResource",
        "rtbfabric:GetCertificateAssociation",
        "rtbfabric:GetInboundExternalLink",
        "rtbfabric:GetLink",
        "rtbfabric:GetLinkRoutingRule",
        "rtbfabric:GetOutboundExternalLink",
        "rtbfabric:GetRequesterGateway",
        "rtbfabric:GetResponderGateway",
        "rtbfabric:ListCertificateAssociations",
        "rtbfabric:ListLinkRoutingRules",
        "rtbfabric:ListLinks",
        "rtbfabric:ListRequesterGateways",
        "rtbfabric:ListResponderGateways",
        "rtbfabric:ListTagsForResource",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
```

```
        "rum:ListAppMonitors",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
```

```
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3:ListTagsForResource",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:GetMetricsConfiguration",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListTagsForResource",
        "s3files:GetAccessPoint",
        "s3files:GetFileSystem",
        "s3files:GetFileSystemPolicy",
        "s3files:GetMountTarget",
        "s3files:GetSynchronizationConfiguration",
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems",
        "s3files:ListMountTargets",
        "s3files:ListTagsForResource",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketMetricsConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:ListTableBuckets",
        "s3tables:ListTagsForResource",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
```

```
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:ListIndexes",
        "s3vectors:ListTagsForResource",
        "s3vectors:ListVectorBuckets",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeClusterSchedulerConfig",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeComputeQuota",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHub",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeMlflowApp",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelCardExportJob",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
```

```
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribePartnerApp",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTrainingPlan",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListClusters",
        "sagemaker:ListClusterSchedulerConfigs",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListComputeQuotas",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHubs",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListLabelingJobs",
```

```
        "sagemaker:ListMlflowApps",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCardExportJobs",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListOptimizationJobs",
        "sagemaker:ListPartnerApps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSpaces",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingPlans",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "sdb:GetAttributes",
```

```
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetTargetDomains",
        "securityagent:GetApplication",
        "securityagent:ListApplications",
        "securityagent:ListPentests",
        "securityagent:ListTagsForResource",
        "securityagent:ListTargetDomains",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetAggregatorV2",
        "securityhub:GetAutomationRuleV2",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:ListAggregatorsV2",
        "securityhub:ListAutomationRulesV2",
        "securityhub:ListConfigurationPolicies",
        "securityhub:ListConfigurationPolicyAssociations",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:ListFindingAggregators",
        "securityhub:ListTagsForResource",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "serviceCatalog:DescribePortfolioShares",
        "servicecatalog:DescribeServiceAction",
        "servicecatalog:DescribeTagOption",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListServiceActions",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
```

```
        "servicecatalog:ListTagOptions",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetAddonInstance",
        "ses:GetAddonSubscription",
        "ses:GetAddressList",
        "ses:GetArchive",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailTemplate",
        "ses:GetIngressPoint",
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:ListAddonInstances",
        "ses:ListAddonSubscriptions",
        "ses:ListAddressLists",
        "ses:ListArchives",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailTemplates",
        "ses:ListIngressPoints",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListRelays",
        "ses:ListRuleSets",
        "ses:ListTagsForResource",
        "ses:ListTemplates",
        "ses:ListTrafficPolicies",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeProtectionGroup",
```

```
        "shield:DescribeSubscription",
        "shield:ListProtectionGroups",
        "shield:ListTagsForResource",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeProtectConfigurations",
        "sms-voice:DescribeSenderIds",
        "sms-voice:GetProtectConfigurationCountryRuleSet",
        "sms-voice:GetResourcePolicy",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:GetRotation",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListRotations",
        "ssm-contacts:ListTagsForResource",
        "ssm-guiconnect:GetConnectionRecordingPreferences",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:ListTagsForResource",
```

```
        "ssm:DescribeAssociation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm:GetAutomationExecution",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetMaintenanceWindow",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:GetServiceSetting",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso:DescribeApplication",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:ListApplications",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineAlias",
        "states:ListActivities",
        "states:ListStateMachineAliases",
        "states:ListStateMachines",
        "states:ListStateMachineVersions",
        "states:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
```

```
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "textract:GetAdapter",
        "textract:ListAdapters",
        "textract:ListTagsForResource",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transcribe:GetCallAnalyticsJob",
        "transcribe:GetVocabularyFilter",
        "transcribe:ListCallAnalyticsJobs",
        "transcribe:ListTagsForResource",
        "transcribe:ListVocabularyFilters",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWebApp",
        "transfer:DescribeWebAppCustomization",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
```

```
        "transfer:ListWebApps",
        "transfer:ListWorkflows",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "verifiedpermissions:ListTagsForResource",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
```

```
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wisdom:GetAIAgent",
        "wisdom:GetAIGuardrail",
        "wisdom:GetAIPrompt",
        "wisdom:GetAssistant",
        "wisdom:ListAIAgentVersions",
        "wisdom:ListAIGuardrails",
        "wisdom:ListAIGuardrailVersions",
        "wisdom:ListAIPromptVersions",
        "wisdom:ListAssistants",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIpAccessSettings",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetIndexingRules",
        "xray:GetSamplingRules",
        "xray:GetTraceSegmentDestination",
        "xray:ListResourcePolicies",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigSLRLogStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "AWSConfigSLRLogEventStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    },
    {
      "Sid" : "AWSConfigSLRApiGatewayStatementID",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes/*",
        "arn:aws:apigateway:*::/v2/apis",
        "arn:aws:apigateway:*::/v2/apis/*",
        "arn:aws:apigateway:*::/v2/apis/*/integrations",
        "arn:aws:apigateway:*::/v2/apis/*/integrations/*"
      ]
```

```
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSConfigThirdPartyServiceRolePolicy

Descrição: Fornece permissões para que o AWS Config faça o inventário e avalie a conformidade de recursos de nuvem de terceiros.

`AWSConfigThirdPartyServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 22 de junho de 2026, 17:57 UTC
- Horário editado: 22 de junho de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigThirdPartyServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGetWebIdentityTokenByConfig",
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "sts:IdentityTokenAudience" : [
            "api://AzureADTokenExchange"
          ]
        }
      }
    },
    {
      "Sid" : "AllowConfigActionsForRules",
      "Effect" : "Allow",
      "Action" : [
        "config:PutEvaluations",
        "config:GetComplianceDetailsByConfigRule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCloudwatchActionsForMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Config"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSConfigUserAccess

Descrição: Fornece acesso para usar o AWS Config, incluindo a pesquisa por tags nos recursos e a leitura de todas as tags. Isso não fornece permissão para configurar o AWS Config, que requer privilégios administrativos.

`AWSConfigUserAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSConfigUserAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de fevereiro de 2015, 19:38 UTC
- Hora da edição: 18 de março de 2019, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConfigUserAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

Conector AWS

Descrição: permite amplo read/write acesso a TODOS os objetos do EC2, read/write acesso a buckets do S3 começando com 'import-to-ec2-' e a capacidade de listar todos os buckets do S3, para que o Connector importe VMs em seu nome. AWS

`AWSConnector` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSConnector` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 11 de fevereiro de 2015, 17:14 UTC
- Hora da edição: 28 de setembro de 2015, 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConnector`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:AbortMultipartUpload",
```

```
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::import-to-ec2-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelConversionTask",
        "ec2:CancelExportTask",
        "ec2:CreateImage",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteTags",
        "ec2:DeleteVolume",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:DetachVolume",
        "ec2:ImportInstance",
        "ec2:ImportVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:CancelImportTask",
        "ec2:ImportSnapshot",
        "ec2:DescribeImportSnapshotTasks"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSControlTowerAccountServiceRolePolicy

Descrição: permite que a AWS Control Tower chame AWS serviços que fornecem configuração automatizada de contas e governança centralizada em seu nome.

`AWSControlTowerAccountServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 05 de junho de 2023, 22:04 UTC
- Horário editado: 20 de maio de 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutRuleOnSpecificSourcesAndDetailTypes",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "events:source" : "aws.securityhub"
        },
        "ForAllValues:StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "Null" : {
          "events:detail-type" : "false"
        },
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowOtherOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
```

```
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowDescribeOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*"
    },
    {
      "Sid" : "AllowControlTowerToPublishSecurityNotifications",
      "Effect" : "Allow",
      "Action" : "sns:publish",
      "Resource" : "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "AllowActionsForSecurityHubIntegration",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:DescribeStandardsControls",
        "securityhub:GetEnabledStandards"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hub/default"
    },
    {
      "Sid" : "AllowDeleteConfigRule",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*"
    },
```

```
    {
      "Sid" : "AllowPutConfigRule",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*"
    },
    {
      "Sid" : "AllowConfigTagResource",
      "Effect" : "Allow",
      "Action" : [
        "config:TagResource"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws-control-tower" : "managed-by-control-tower"
        }
      }
    },
    {
      "Sid" : "AllowConfigRulesDescribe",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowControlTowerToCreateConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigurationAggregator"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "AllowControlTowerToManageConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
        "config:DescribeAggregateComplianceByConfigRules",
        "config:SelectAggregateResourceConfig"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/config-aggregator-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowControlTowerToTagConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
        "config:TagResource"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws-control-tower" : "managed-by-control-tower",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowControlTowerToPassAggregatorRoleToConfig",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "config.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeConfigurationAggregators",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationAggregators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowListDelegatedAdministratorsForConfig",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowListDescribeOrganization",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "AllowActionsForCloudFormationHooksIntegration",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:SetTypeConfiguration",
        "cloudformation:DeactivateType",
        "cloudformation:ActivateType"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:type/hook/AWS-ControlTower*"
    },
    {
      "Sid" : "AllowBatchDescribeTypeConfigurationsForHookConfigFetch",
      "Effect" : "Allow",
      "Action" : "cloudformation:BatchDescribeTypeConfigurations",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSControlTowerCloudTrailRolePolicy

Descrição: A Torre de AWS AWS CloudTrail Controle é uma prática recomendada e fornece essa função para AWS CloudTrail. AWS CloudTrail assume essa função para criar e publicar registros CloudTrail

`AWSControlTowerCloudTrailRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSControlTowerCloudTrailRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço

- Horário de criação: 05 de novembro de 2025, 21:19 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerCloudTrailRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogStream",
      "Resource" : "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs*:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSControlTowerIdentityCenterManagementPolicy

Descrição: fornece permissões para gerenciar os recursos do IAM Identity Center (IdC) nas contas membros inscritas na AWS Control Tower. A política é anexada à AWSControlTowerAdmin função somente se o cliente tiver optado pela integração do IAM IdC em sua AWS Control Tower Landing Zone.

`AWSControlTowerIdentityCenterManagementPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSControlTowerIdentityCenterManagementPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 03 de outubro de 2025, 18:34 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerIdentityCenterManagementPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowIdentityCenterInstancePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sso:ListPermissionSets"
      ],
      "Resource" : "arn:aws:sso:::instance/*"
    },
    {
      "Sid" : "AllowIdentityCenterManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations",
        "sso:ListProfileAssociations",
        "sso:AssociateProfile",
        "sso:GetProfile",
        "sso:CreateProfile",
        "sso:UpdateProfile",
        "sso:GetTrust",
        "sso:CreateTrust",
        "sso:UpdateTrust",
        "sso:CreateApplicationInstance",
        "sso:GetApplicationInstance",
        "sso:GetSSOStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowIdentityCenterDirectoryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:SearchGroups",
        "sso-directory:CreateGroup",
        "sso-directory:SearchUsers",
        "sso-directory:CreateUser",
        "sso-directory:DescribeDirectory"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSControlTowerServiceRolePolicy

Descrição: Fornece acesso aos AWS recursos gerenciados ou usados pela AWS Control Tower

`AWSControlTowerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSControlTowerServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 03 de maio de 2019, 18:19 UTC
- Horário editado: 10 de setembro de 2026, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`

Versão da política

Versão da política: v22 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateStackInstances",
```

```
        "cloudformation:CreateStackSet",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateStackInstances",
        "cloudformation:UpdateStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackInstances",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateStackInstances",
        "cloudformation:UpdateStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
        "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateTrail",
        "cloudtrail:DeleteTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudtrail:UpdateTrail",
        "cloudtrail:PutEventSelectors",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs*:*",
        "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-controltower*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSControlTowerExecution",
        "arn:aws:iam::*:role/AWSControlTowerBlueprintAccess"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "ec2:DescribeAvailabilityZones",
        "iam:ListRoles",
        "logs:CreateLogGroup",
```

```
        "logs:DescribeLogGroups",
        "organizations:CreateAccount",
        "organizations:DescribeAccount",
        "organizations:DescribeCreateAccountStatus",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListRoots",
        "organizations:MoveAccount",
        "servicecatalog:AssociatePrincipalWithPortfolio"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListAttachedRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
        "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
        "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
        "config:PutConfigurationAggregator",
        "config:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/aws-control-tower" : "managed-by-control-tower"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "config.amazonaws.com",
            "cloudtrail.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "account:EnableRegion",
        "account:ListRegions",
```

```
        "account:GetRegionOptStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFormationHooksIntegration",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:SetTypeConfiguration",
        "cloudformation:DeactivateType",
        "cloudformation:ActivateType"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:type/hook/AWS-ControlTower*"
    },
    {
      "Sid" : "AllowBatchDescribeTypeConfigurationsForHookConfigFetch",
      "Effect" : "Allow",
      "Action" : "cloudformation:BatchDescribeTypeConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFormationStackSetOrganizationsTrustedAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ActivateOrganizationsAccess",
        "cloudformation:DescribeOrganizationsAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role",
        "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
        "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSCostAndUsageReportAutomationPolicy

Descrição: concede permissões para descrever a organização da conta, criar buckets do S3 para o programa MAP e aplicar tags a ele, criar um relatório de custo e uso e descrever as definições do Relatório de Custos e Uso.

`AWSCostAndUsageReportAutomationPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSCostAndUsageReportAutomationPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 01 de novembro de 2021, 21:27 UTC
- Hora da edição: 01 de novembro de 2021, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketTagging",
        "s3:PutBucketTagging",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:CreateBucket"
      ],
      "Resource" : "arn:aws:s3:::aws-map-cur-bucket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cur:PutReportDefinition",
        "cur:DeleteReportDefinition",
        "cur:DescribeReportDefinitions"
      ],
      "Resource" : "arn:aws:cur:*:*:definition/map-migrated-report"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "cur:DescribeReportDefinitions",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDataExchangeDataGrantOwnerFullAccess

Descrição: dá aos proprietários do Data Grant acesso às ações do AWS Data Exchange usando o Console de gerenciamento da AWS SDK e.

`AWSDataExchangeDataGrantOwnerFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDataExchangeDataGrantOwnerFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de outubro de 2024, 14:43 UTC
- Hora da edição: 24 de outubro de 2024, 14:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeDataGrantOwnerFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateDataSet",
        "dataexchange:UpdateDataSet",
        "dataexchange:GetDataSet",
        "dataexchange:DeleteDataSet",
        "dataexchange:ListDataSets",
        "dataexchange:CreateRevision",
        "dataexchange:UpdateRevision",
        "dataexchange:GetRevision",
        "dataexchange:DeleteRevision",
        "dataexchange:RevokeRevision",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:CreateAsset",
        "dataexchange:UpdateAsset",
        "dataexchange:GetAsset",
        "dataexchange:DeleteAsset",
        "dataexchange:ListRevisionAssets",
        "dataexchange:SendApiAsset",
        "dataexchange:CreateDataGrant",
        "dataexchange:GetDataGrant",
        "dataexchange:DeleteDataGrant",
        "dataexchange:ListDataGrants",
        "dataexchange:PublishToDataGrant",
        "dataexchange:SendDataSetNotification",
        "dataexchange:TagResource",
        "dataexchange:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeJobsActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "IMPORT_ASSETS_FROM_S3",
            "IMPORT_ASSET_FROM_SIGNED_URL",
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "IMPORT_ASSET_FROM_API_GATEWAY_API",
            "IMPORT_ASSETS_FROM_REDSHIFT_DATA_SHARES",
            "IMPORT_ASSETS_FROM_LAKE_FORMATION_TAG_POLICY"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDataExchangeDataGrantReceiverFullAccess

Descrição: Fornece ao destinatário do AWS Data Grant acesso às ações do Data Exchange usando o Console de gerenciamento da AWS SDK e.

`AWSDataExchangeDataGrantReceiverFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDataExchangeDataGrantReceiverFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de outubro de 2024, 14:45 UTC
- Hora da edição: 24 de outubro de 2024, 14:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeDataGrantReceiverFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetDataSet",
        "dataexchange:ListDataSets",
        "dataexchange:GetRevision",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:GetAsset",
        "dataexchange:ListRevisionAssets",
        "dataexchange:SendApiAsset"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "DataExchangeExportActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "EXPORT_REVISIONS_TO_S3"
          ]
        }
      }
    },
    {
      "Sid" : "DataExchangeEventActionActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateEventAction",
        "dataexchange:UpdateEventAction",
        "dataexchange:DeleteEventAction",
        "dataexchange:GetEventAction",
        "dataexchange:ListEventActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeDataGrantActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:AcceptDataGrant",
        "dataexchange:ListReceivedDataGrants",
        "dataexchange:GetReceivedDataGrant"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDataExchangeFullAccess

Descrição: Concede acesso total ao intercâmbio de AWS dados e AWS Marketplace às ações usando o Console de gerenciamento da AWS SDK e. Ele também fornece acesso selecionado aos serviços relacionados necessários para aproveitar ao máximo o intercâmbio de AWS dados.

`AWSDataExchangeFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDataExchangeFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 13 de novembro de 2019, 19:27 UTC
- Hora da edição: 24 de junho de 2024, 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeFullAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3GetActionConditionalTagAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3WriteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
```

```
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceProviderActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms",
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AWSMarketplaceSubscriberActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListPrivateListings",
        "aws-marketplace:DescribeAgreement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftConditionalActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Sid" : "RedshiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayActions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDataExchangeProviderFullAccess

Descrição: Concede ao provedor de dados acesso ao intercâmbio de AWS dados e AWS Marketplace às ações usando o Console de gerenciamento da AWS SDK e. Ele também fornece acesso selecionado aos serviços relacionados necessários para aproveitar ao máximo o intercâmbio de AWS dados.

`AWSDataExchangeProviderFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDataExchangeProviderFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 13 de novembro de 2019, 19:27 UTC

- Hora da edição: 15 de agosto de 2024, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateDataSet",
        "dataexchange:CreateRevision",
        "dataexchange:CreateAsset",
        "dataexchange:Get*",
        "dataexchange:Update*",
        "dataexchange:List*",
        "dataexchange:Delete*",
        "dataexchange:TagResource",
        "dataexchange:UntagResource",
        "dataexchange:PublishDataSet",
        "dataexchange:SendApiAsset",
        "dataexchange:RevokeRevision",
        "dataexchange:SendDataSetNotification",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeJobsActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "IMPORT_ASSETS_FROM_S3",
            "IMPORT_ASSET_FROM_SIGNED_URL",
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "IMPORT_ASSET_FROM_API_GATEWAY_API",
            "IMPORT_ASSETS_FROM_REDSHIFT_DATA_SHARES"
          ]
        }
      }
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3GetActionConditionalTagAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "S3WriteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
```

```
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftConditionalActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Sid" : "RedshiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayActions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDataExchangeReadOnly

Descrição: Concede acesso somente para leitura ao intercâmbio AWS de dados e às AWS Marketplace ações usando o SDK Console de gerenciamento da AWS e.

`AWSDataExchangeReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDataExchangeReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 13 de novembro de 2019, 19:27 UTC
- Hora da edição: 24 de outubro de 2024, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeReadOnly`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetAsset",
        "dataexchange:GetDataSet",
        "dataexchange:GetEventAction",
        "dataexchange:GetJob",
        "dataexchange:GetRevision",
        "dataexchange:GetDataGrant",
        "dataexchange:GetReceivedDataGrant",
        "dataexchange:ListDataGrants",
        "dataexchange:ListReceivedDataGrants",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:ListDataSets",
        "dataexchange:ListEventActions",
        "dataexchange:ListJobs",
        "dataexchange:ListRevisionAssets",
        "dataexchange:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms",
        "aws-marketplace:ListPrivateListings",
```

```
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDataExchangeServiceRolePolicyForLicenseManagement

Descrição: Permite que o AWS Data Exchange acesse Serviços da AWS os recursos usados ou gerenciados pelo AWS Data Exchange para gerenciamento de licenças.

`AWSDataExchangeServiceRolePolicyForLicenseManagement` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 10 de outubro de 2024, 14:54 UTC
- Hora da edição: 10 de outubro de 2024, 14:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataExchangeServiceRolePolicyForLicenseManagement`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowLicenseManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "license-manager:ListDistributedGrants",
        "license-manager:GetGrant",
        "license-manager:CreateGrantVersion",
        "license-manager:DeleteGrant"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDataExchangeServiceRolePolicyForOrganizationDiscovery

Descrição: permite que o AWS Data Exchange leia dados sobre sua AWS organização para determinar a elegibilidade para a distribuição de licenças de concessões de AWS dados do Data Exchange.

`AWSDataExchangeServiceRolePolicyForOrganizationDiscovery` é uma [política gerenciada pelo AWS].

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 10 de outubro de 2024, 14:33 UTC
- Hora da edição: 10 de outubro de 2024, 14:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataExchangeServiceRolePolicyForOrganizationDiscovery`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAWSOrganizationsActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
```

```
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDataExchangeSubscriberFullAccess

Descrição: Concede ao assinante de dados acesso ao intercâmbio de AWS dados e AWS Marketplace às ações usando o SDK Console de gerenciamento da AWS e. Ele também fornece acesso selecionado aos serviços relacionados necessários para aproveitar ao máximo o intercâmbio de AWS dados.

`AWSDataExchangeSubscriberFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDataExchangeSubscriberFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 13 de novembro de 2019, 19:27 UTC
- Hora da edição: 21 de maio de 2024, 17:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:Get*",
        "dataexchange:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeExportActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "EXPORT_REVISIONS_TO_S3"
          ]
        }
      }
    },
    {
      "Sid" : "DataExchangeEventActionActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateEventAction",
        "dataexchange:UpdateEventAction",
```

```
        "dataexchange:DeleteEventAction",
        "dataexchange:SendApiAsset"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceSubscriberActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDataLifecycleManagerServiceRole

Descrição: Fornece permissões apropriadas ao AWS Data Lifecycle Manager para realizar ações sobre os recursos AWS

`AWSDataLifecycleManagerServiceRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDataLifecycleManagerServiceRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 06 de julho de 2018, 19:34 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:EnableFastSnapshotRestores",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DisableFastSnapshotRestores",
        "ec2:CopySnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:ModifySnapshotTier",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-cwe.*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDataLifecycleManagerServiceRoleForAMIManagement

Descrição: Fornece permissões apropriadas ao AWS Data Lifecycle Manager para realizar ações em AWS recursos para gerenciamento de AMI

`AWSDataLifecycleManagerServiceRoleForAMIManagement` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDataLifecycleManagerServiceRoleForAMIManagement` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 21 de outubro de 2020, 19:39 UTC

- Hora da edição: 19 de agosto de 2021, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ResetImageAttribute",
        "ec2:DeregisterImage",
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImageDeprecation",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDataLifecycleManagerSSMFullAccess

Descrição: fornece ao Amazon Data Lifecycle Manager permissão para realizar as ações do Systems Manager necessárias para executar scripts prévios e posteriores em todas as instâncias do Amazon EC2.

`AWSDataLifecycleManagerSSMFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDataLifecycleManagerSSMFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 31 de outubro de 2023, 20:29 UTC
- Hora da edição: 16 de novembro de 2023, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTaggedSSMDocumentsOnly",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DLMScriptsAccess" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSpecificAWSOwnedSSMDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ssm:*:*:document/AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA"
      ]
    },
    {
      "Sid" : "AllowAllEC2Instances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDataPipeline_FullAccess

Descrição: fornece acesso total ao Data Pipeline, acesso à lista para perfis do S3, DynamoDB, Redshift, RDS, SNS e IAM e acesso passRole para perfis padrão.

`AWSDataPipeline_FullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDataPipeline_FullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 19 de janeiro de 2017, 23:14 UTC
- Hora da edição: 17 de agosto de 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:List*",
```

```
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/DataPipelineDefaultRole"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDataPipeline_PowerUser

Descrição: fornece acesso total ao Data Pipeline, acesso à lista para perfis do S3, DynamoDB, Redshift, RDS, SNS e IAM e acesso passRole para perfis padrão.

`AWSDataPipeline_PowerUser` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDataPipeline_PowerUser` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 19 de janeiro de 2017, 23:16 UTC
- Hora da edição: 17 de agosto de 2017, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:List*",
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles",
        "datapipeline:*"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/DataPipelineDefaultRole"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDataSyncDiscoveryServiceRolePolicy

Descrição: permite que o DataSync Discovery se integre a outros AWS serviços em seu nome.

`AWSDataSyncDiscoveryServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Hora da criação: 20 de março de 2023, 22:19 UTC
- Hora da edição: 20 de março de 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync:log-stream:*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDataSyncFullAccess

Descrição: AWS DataSync Fornece acesso total e acesso mínimo às suas dependências

`AWSDataSyncFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDataSyncFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de janeiro de 2019, 19:40 UTC
- Horário editado: 12 de fevereiro de 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncFullAccess`

Versão da política

Versão da política: v16 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataSyncFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datasync:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "iam:GetRole",
        "iam:ListRoles",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "outposts:ListOutposts",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListRegionalBuckets",
        "secretsmanager:ListSecrets",
        "kms:ListAliases",
        "kms:DescribeKey"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataSyncPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "datasync.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DataSyncCreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/datasync.amazonaws.com/
AWSServiceRoleForDataSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "datasync.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataSyncSecretsManagerCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "DataSyncSecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "aws-
datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDataSyncReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao AWS DataSync

`AWSDataSyncReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDataSyncReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de janeiro de 2019, 19:18 UTC
- Hora da edição: 30 de junho de 2020, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:Describe*",
        "datasync:List*",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "iam:GetRole",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDataSyncServiceRolePolicy

Descrição: Permite DataSync a integração com outros AWS serviços em seu nome

`AWSDataSyncServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 9 de outubro de 2024, 17:45 UTC
- Horário editado: 15 de abril de 2025, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataSyncCloudWatchLogCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*"
      ]
    },
    {
      "Sid" : "DataSyncCloudWatchLogStreamUpdateAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*:log-stream:*"
      ]
    },
    {
      "Sid" : "DataSyncSecretsManagerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "aws-
datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDeadlineCloud-FleetWorker

Descrição: Fornece aos funcionários do AWS Deadline Cloud acesso para executar tarefas em uma fazenda.

`AWSDeadlineCloud-FleetWorker` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDeadlineCloud-FleetWorker` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 1º de abril de 2024, 17:21 UTC
- Hora da edição: 1º de abril de 2024, 17:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-FleetWorker`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunTasksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForWorker",
        "deadline:UpdateWorker",
        "deadline:UpdateWorkerSchedule",
        "deadline:BatchGetJobEntity",
        "deadline:AssumeQueueRoleForWorker"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDeadlineCloud-UserAccessFarms

Descrição: fornece acesso à estação de trabalho do usuário às fazendas do AWS Deadline Cloud com Read-Only permissões limitadas para chamar outros serviços necessários. Anexe esta política ao perfil de usuário associado ao seu estúdio.

`AWSDeadlineCloud-UserAccessFarms` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDeadlineCloud-UserAccessFarms` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 1º de abril de 2024, 16:54 UTC
- Horário editado: 29 de maio de 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFarms`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "deadline:GetMonitorSettings",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "deadline:AssociateMemberToFarm",
        "deadline:AssociateMemberToFleet",
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue",
        "deadline:CreateBudget",
        "deadline:DeleteBudget",
        "deadline:DisassociateMemberFromFarm",
        "deadline:DisassociateMemberFromFleet",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue",
        "deadline:GetBudget",
        "deadline:GetSessionsStatisticsAggregation",
        "deadline:ListBudgets",
        "deadline:StartSessionsStatisticsAggregation",
        "deadline:UpdateBudget"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFarm",
        "deadline:AssociateMemberToFleet",
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "MANAGER"
          ]
```

```
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromFarm",
        "deadline:DisassociateMemberFromFleet",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
```

```
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFarmMembers",
        "deadline:ListFleetMembers",
        "deadline:ListJobMembers",
        "deadline:ListQueueMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerContributorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForUser",
        "deadline:CreateJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForRead",
        "deadline:AssumeQueueRoleForRead",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetJob",
        "deadline:GetJobTemplate",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetStorageProfile",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:GetVolume",
        "deadline:GetWorker",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListSessionsForWorker",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfiles",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTasks",
        "deadline:ListVolumes",
        "deadline:ListWorkers",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks",
        "deadline:SearchWorkers"
      ],
      "Resource" : [
        "*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListJobs",
        "deadline:ListQueues"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDeadlineCloud-UserAccessFleets

Descrição: Fornece ao usuário acesso à estação de trabalho das frotas do AWS Deadline Cloud com Read-Only permissões limitadas para ligar para outros serviços necessários. Anexe esta política ao perfil de usuário associado ao seu estúdio.

`AWSDeadlineCloud-UserAccessFleets` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDeadlineCloud-UserAccessFleets` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 1º de abril de 2024, 17:01 UTC
- Horário editado: 29 de maio de 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFleets`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFleet",
        "deadline:DisassociateMemberFromFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFleetMembers"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForRead",
        "deadline:GetFleet",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetVolume",
        "deadline:GetWorker",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionsForWorker",
        "deadline:ListVolumes",
        "deadline:ListWorkers",
        "deadline:SearchWorkers"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFleets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDeadlineCloud-UserAccessJobs

Descrição: Fornece ao usuário acesso à estação de trabalho do usuário às tarefas do AWS Deadline Cloud com Read-Only permissões limitadas para chamar outros serviços necessários. Anexe esta política ao perfil de usuário associado ao seu estúdio.

`AWSDeadlineCloud-UserAccessJobs` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDeadlineCloud-UserAccessJobs` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 1º de abril de 2024, 17:05 UTC
- Hora da edição: 7 de outubro de 2024, 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessJobs`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:DisassociateMemberFromJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "MANAGER"
          ]
        },
```

```
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:GetJob",
        "deadline:GetJobTemplate",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetTask",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListSessionActions",
```

```
        "deadline:ListSessions",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListTasks",
        "deadline:SearchSteps",
        "deadline:SearchTasks"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobs"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDeadlineCloud-UserAccessQueues

Descrição: fornece acesso à estação de trabalho do usuário às filas do AWS Deadline Cloud com Read-Only permissões limitadas para chamar outros serviços necessários. Anexe esta política ao perfil de usuário associado ao seu estúdio.

`AWSDeadlineCloud-UserAccessQueues` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDeadlineCloud-UserAccessQueues` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 1º de abril de 2024, 17:10 UTC
- Hora da edição: 7 de outubro de 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessQueues`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue"
      ],
      "Resource" : [
        "*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
```

```
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobMembers",
        "deadline:ListQueueMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerContributorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForUser",
        "deadline:CreateJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForRead",
        "deadline:GetJob",
        "deadline:GetJobTemplate",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTasks",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobs",
        "deadline:ListQueues"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDeadlineCloud-WorkerHost

Descrição: Fornece acesso para que os anfitriões de funcionários do AWS Deadline Cloud se juntem a uma frota em uma fazenda.

`AWSDeadlineCloud-WorkerHost` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDeadlineCloud-WorkerHost` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 1º de abril de 2024, 17:28 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "JoinFleetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:CreateWorker",
        "deadline:AssumeFleetRoleForWorker"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "TagWorkerPermission",
      "Effect" : "Allow",
      "Action" : [
        "deadline:TagResource"
      ],
```

```
      "Resource" : "arn:aws:deadline:*:*:farm/*/fleet/*/worker/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}",
          "deadline:CalledAction" : "CreateWorker"
        }
      }
    },
    {
      "Sid" : "ListFleetTagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListTagsForResource"
      ],
      "Resource" : "arn:aws:deadline:*:*:farm/*/fleet/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}",
          "deadline:CalledAction" : "CreateWorker"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDeepLensLambdaFunctionAccessPolicy

Descrição: Essa política especifica as permissões exigidas pelas funções DeepLens administrativas lambda que são executadas em um dispositivo DeepLens

`AWSDeepLensLambdaFunctionAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDeepLensLambdaFunctionAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2017, 15:47 UTC
- Hora da edição: 11 de junho de 2019, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepLensS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*/*",
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensGreenGrassCloudWatchAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
    },
    {
      "Sid" : "DeepLensAccess",
      "Effect" : "Allow",
      "Action" : [
        "deeplens:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDeepLensServiceRolePolicy

Descrição: Concede AWS DeepLens acesso aos Serviços da AWS recursos e funções necessários para DeepLens e suas dependências, incluindo IoT, S3 e Lambda. GreenGrass AWS

`AWSDeepLensServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDeepLensServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 29 de novembro de 2017, 15:46 UTC
- Hora da edição: 25 de setembro de 2019, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepLensIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
```

```
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "DeepLensIoTCreateCertificateAndPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensIoTAttachCertificatePolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/deeplens*",
        "arn:aws:iot:*:*:cert/*"
      ]
```

```
    },
    {
      "Sid" : "DeepLensIoTDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:GetThingShadow",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensAccess",
      "Effect" : "Allow",
      "Action" : [
        "deeplens:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensS3Buckets",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucket",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensCreateS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensIAMPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "greengrass.amazonaws.com",
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DeepLensIAMLambdaPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/AWSDeepLens*",
        "arn:aws:iam::*:role/service-role/AWSDeepLens*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DeepLensGreenGrassAccess",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:AssociateRoleToGroup",
        "greengrass:AssociateServiceRoleToAccount",
        "greengrass:CreateResourceDefinition",
        "greengrass:CreateResourceDefinitionVersion",
        "greengrass:CreateCoreDefinition",
        "greengrass:CreateCoreDefinitionVersion",
        "greengrass:CreateDeployment",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:CreateGroup",
        "greengrass:CreateGroupCertificateAuthority",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateLoggerDefinition",
        "greengrass:CreateLoggerDefinitionVersion",
        "greengrass:CreateSubscriptionDefinition",
        "greengrass:CreateSubscriptionDefinitionVersion",
        "greengrass:DeleteCoreDefinition",
        "greengrass:DeleteFunctionDefinition",
        "greengrass:DeleteGroup",
        "greengrass:DeleteLoggerDefinition",
        "greengrass:DeleteSubscriptionDefinition",
        "greengrass:DisassociateRoleFromGroup",
        "greengrass:DisassociateServiceRoleFromAccount",
        "greengrass:GetAssociatedRole",
        "greengrass:GetConnectivityInfo",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetDeviceDefinition",
        "greengrass:GetDeviceDefinitionVersion",
        "greengrass:GetFunctionDefinition",
```

```
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupCertificateAuthority",
        "greengrass:GetGroupCertificateConfiguration",
        "greengrass:GetGroupVersion",
        "greengrass:GetLoggerDefinition",
        "greengrass:GetLoggerDefinitionVersion",
        "greengrass:GetResourceDefinition",
        "greengrass:GetServiceRoleForAccount",
        "greengrass:GetSubscriptionDefinition",
        "greengrass:GetSubscriptionDefinitionVersion",
        "greengrass:ListCoreDefinitionVersions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeployments",
        "greengrass:ListDeviceDefinitionVersions",
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitionVersions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroupCertificateAuthorities",
        "greengrass:ListGroupVersions",
        "greengrass:ListGroups",
        "greengrass:ListLoggerDefinitionVersions",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListSubscriptionDefinitionVersions",
        "greengrass:ListSubscriptionDefinitions",
        "greengrass:ResetDeployments",
        "greengrass:UpdateConnectivityInfo",
        "greengrass:UpdateCoreDefinition",
        "greengrass:UpdateDeviceDefinition",
        "greengrass:UpdateFunctionDefinition",
        "greengrass:UpdateGroup",
        "greengrass:UpdateGroupCertificateConfiguration",
        "greengrass:UpdateLoggerDefinition",
        "greengrass:UpdateSubscriptionDefinition",
        "greengrass:UpdateResourceDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensLambdaAdminFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensLambdaUsersFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "DeepLensSageMakerWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:StopTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensSageMakerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
```

```
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:DeleteStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/deeplens*/*"
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDeepRacerAccountAdminAccess

Descrição: acesso DeepRacer administrativo a todas as ações, incluindo alternar entre o modo multiusuário e o modo de usuário único.

`AWSDeepRacerAccountAdminAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDeepRacerAccountAdminAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de outubro de 2021, 1:27 UTC
- Hora da edição: 28 de outubro de 2021, 1:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
```

```
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDeepRacerCloudFormationAccessPolicy

Descrição: Permite CloudFormation criar e gerenciar AWS pilhas e recursos em seu nome.

`AWSDeepRacerCloudFormationAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDeepRacerCloudFormationAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de fevereiro de 2019, 21:59 UTC
- Hora da edição: 14 de junho de 2019, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
```

```
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachInternetGateway",
        "ec2:DisassociateRouteTable",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/AWSDeepRacerLambdaAccessRole",
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:GetFunction",
        "lambda:DeleteFunction",
        "lambda:TagResource",
        "lambda:UpdateFunctionCode"
```

```
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*DeepRacer*",
        "arn:aws:lambda:*:*:function:*Deepracer*",
        "arn:aws:lambda:*:*:function:*deepracer*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:DeleteBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:CreateSimulationApplication",
        "robomaker:CreateSimulationApplicationVersion",
        "robomaker:DeleteSimulationApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListSimulationApplications",
        "robomaker:TagResource",
        "robomaker:UpdateSimulationApplication"
      ],
      "Resource" : [
        "arn:aws:robomaker:*:*:/createSimulationApplication",
        "arn:aws:robomaker:*:*:simulation-application/deepracer*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDeepRacerDefaultMultiUserAccess

Descrição: Acesso DeepRacer MultiUser padrão do usuário para usar o deepracer no modo multiusuário

`AWSDeepRacerDefaultMultiUserAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDeepRacerDefaultMultiUserAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de outubro de 2021, 1:27 UTC
- Hora da edição: 28 de outubro de 2021, 1:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:Add*",
        "deepracer:Remove*",
        "deepracer:Create*",
        "deepracer:Perform*",
        "deepracer:Clone*",
        "deepracer:Get*",
        "deepracer:List*",
        "deepracer:Edit*",
        "deepracer:Start*",
        "deepracer:Set*",
        "deepracer:Update*",
        "deepracer:Delete*",
        "deepracer:Stop*",
        "deepracer:Import*",
        "deepracer:Tag*",
        "deepracer:Untag*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "false"
        },
        "Bool" : {
          "deepracer:MultiUser" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:GetAccountConfig",
        "deepracer:GetTrack",
        "deepracer:ListTracks",
        "deepracer:TestRewardFunction"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "deepracer:Admin*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDeepRacerFullAccess

Descrição: Fornece acesso total AWS DeepRacer a. Também fornece acesso seletivo aos serviços relacionados (por exemplo, S3).

`AWSDeepRacerFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDeepRacerFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 05 de outubro de 2020, 22:03 UTC
- Hora da edição: 05 de outubro de 2020, 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*",
        "arn:aws:s3:::*DeepRacer*/*",
        "arn:aws:s3:::*Deepracer*/*",
        "arn:aws:s3:::*deepracer*/*",
        "arn:aws:s3:::dr-*/*"
```

```
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDeepRacerRoboMakerAccessPolicy

Descrição: Permite RoboMaker criar os recursos necessários e chamar AWS os serviços em seu nome.

`AWSDeepRacerRoboMakerAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDeepRacerRoboMakerAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de fevereiro de 2019, 21:59 UTC
- Hora da edição: 28 de fevereiro de 2019, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs",
        "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs:log-stream:*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/DeepRacer" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:TagStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/dr-*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDeepRacerServiceRolePolicy

Descrição: Permite DeepRacer criar os recursos necessários e chamar AWS os serviços em seu nome.

`AWSDeepRacerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDeepRacerServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 28 de fevereiro de 2019, 21:58 UTC
- Hora da edição: 12 de junho de 2019, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:*",
        "sagemaker:*",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DetectStackDrift",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:DescribeStackResourceDrifts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      },
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSDeepRacer*",
        "arn:aws:iam::*:role/service-role/AWSDeepRacer*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*DeepRacer*",
        "arn:aws:lambda:*:*:function:*Deepracer*",
        "arn:aws:lambda:*:*:function:*deepracer*",
        "arn:aws:lambda:*:*:function:*dr-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:DeleteObject",
        "s3:ListBucket",
```

```
        "s3:PutObject",
        "s3:PutBucketPolicy",
        "s3:GetBucketAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/DeepRacer" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DeleteStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:GetHLSStreamingSessionURL",
        "kinesisvideo:GetMedia",
        "kinesisvideo:PutMedia",
        "kinesisvideo:TagStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/dr-*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDenyAll

Descrição: negar todo o acesso.

`AWSDenyAll` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDenyAll` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de maio de 2019, 22:36 UTC
- Hora da edição: 18 de dezembro de 2023, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDenyAll`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "DenyAll",
      "Effect" : "Deny",
      "Action" : [
        "*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDeviceFarmFullAccess

Descrição: Fornece acesso total a todas as operações AWS do Device Farm.

`AWSDeviceFarmFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDeviceFarmFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 13 de julho de 2015, 16:37 UTC
- Hora da edição: 13 de julho de 2015, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "devicefarm:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDeviceFarmServiceRolePolicy

Descrição: Conceda permissões ao AWS Device Farm para chamar as APIs de rede do EC2 em seu nome.

`AWSDeviceFarmServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 20 de setembro de 2022, 21:02 UTC
- Hora da edição: 20 de setembro de 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDeviceFarmTestGridServiceRolePolicy

Descrição: Conceda permissões ao AWS Device Farm para chamar as APIs do EC2 em seu nome.

`AWSDeviceFarmTestGridServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Hora da criação: 26 de maio de 2021, 22:01 UTC
- Hora da edição: 26 de maio de 2021, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDirectConnectFullAccess

Descrição: Fornece acesso total ao AWS Direct Connect por meio do Console de gerenciamento da AWS.

`AWSDirectConnectFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDirectConnectFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 30 de abril de 2019, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDirectConnectReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao AWS Direct Connect por meio do Console de gerenciamento da AWS.

`AWSDirectConnectReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDirectConnectReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 18 de maio de 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDirectConnectServiceRolePolicy

Descrição: Fornece permissão ao AWS Direct Connect para criar e gerenciar AWS recursos em seu nome.

`AWSDirectConnectServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 14 de janeiro de 2021, 18:35 UTC
- Hora da edição: 14 de janeiro de 2021, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDirectoryServiceDataFullAccess

Descrição: Fornece acesso total aos dados AWS do serviço de diretório.

`AWSDirectoryServiceDataFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDirectoryServiceDataFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de setembro de 2024, 21:45 UTC

- Hora da edição: 18 de setembro de 2024, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceDataFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSDataFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:AccessDSData",
        "ds-data:AddGroupMember",
        "ds-data:CreateGroup",
        "ds-data:CreateUser",
        "ds-data:DeleteGroup",
        "ds-data:DeleteUser",
        "ds-data:DescribeGroup",
        "ds-data:DescribeUser",
        "ds-data:DisableUser",
        "ds-data:ListGroupMembers",
        "ds-data:ListGroups",
        "ds-data:ListGroupsForMember",
        "ds-data:ListUsers",
        "ds-data:RemoveGroupMember",
        "ds-data:SearchGroups",
        "ds-data:SearchUsers",
        "ds-data:UpdateGroup",
        "ds-data:UpdateUser"
      ],
      "Resource" : [
        "arn:aws:ds:*:*:directory/*"
```

```
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDirectoryServiceDataReadOnlyAccess

Descrição: Fornece acesso somente para leitura aos dados do serviço de AWS diretório

`AWSDirectoryServiceDataReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDirectoryServiceDataReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de setembro de 2024, 22:00 UTC
- Hora da edição: 18 de setembro de 2024, 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceDataReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSDataReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:AccessDSData",
        "ds-data:DescribeGroup",
        "ds-data:DescribeUser",
        "ds-data:ListGroupMembers",
        "ds-data:ListGroups",
        "ds-data:ListGroupsForMember",
        "ds-data:ListUsers",
        "ds-data:SearchGroups",
        "ds-data:SearchUsers"
      ],
      "Resource" : [
        "arn:aws:ds:*:*:directory/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDirectoryServiceFullAccess

Descrição: Fornece acesso total ao AWS Directory Service.

`AWSDirectoryServiceFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDirectoryServiceFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 2 de abril de 2024, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectoryServiceFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
```

```
        "ec2:DescribeSecurityGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "iam:ListRoles",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DirectoryServiceEventTopic",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:DirectoryMonitoring*"
    },
    {
      "Sid" : "DirectoryServiceOrganizations",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "ds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DirectoryServiceTags",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDirectoryServiceReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao AWS Directory Service.

`AWSDirectoryServiceReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDirectoryServiceReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 25 de setembro de 2018, 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDirectoryServiceServiceRolePolicy

Descrição: política para a função vinculada ao serviço do Directory Service.

`AWSDirectoryServiceServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 11 de julho de 2025, 00:22 UTC
- Horário editado: 11 de julho de 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectoryServiceServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "SSMSendCommandPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "EC2DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDiscoveryContinuousExportFirehosePolicy

Descrição: Fornece acesso de gravação aos AWS recursos necessários para o AWS Discovery Continuous Export

`AWSDiscoveryContinuousExportFirehosePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSDiscoveryContinuousExportFirehosePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de agosto de 2018, 18:29 UTC
- Hora da edição: 08 de junho de 2021, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTableVersions"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-application-discovery-service-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/firehose:log-
stream:*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDMSFleetAdvisorServiceRolePolicy

Descrição: permite que o DMS Fleet Advisor gerencie CloudWatch métricas em seu nome.

`AWSDMSFleetAdvisorServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 6 de março de 2023, 9:10 UTC
- Hora da edição: 6 de março de 2023, 9:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/DMS/FleetAdvisor"
      }
    }
  }
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSDMSServerlessServiceRolePolicy

Descrição: Concede ao AWS DMS permissões sem servidor para criar e gerenciar recursos do DMS em sua conta em seu nome

`AWSDMSServerlessServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 18 de maio de 2023, 20:28 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "id0",
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dms:req-tag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id1",
      "Effect" : "Allow",
      "Action" : [
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "id2",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTask",
        "dms:StopReplicationTask",
        "dms:ModifyReplicationTask",
        "dms:DeleteReplicationTask",
        "dms:ModifyReplicationInstance",
        "dms:DeleteReplicationInstance"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:task:*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/ResourceCreatedBy" : "DMSServerless"
        }
      }
```

```
    },
    {
      "Sid" : "id3",
      "Effect" : "Allow",
      "Action" : [
        "dms:TestConnection",
        "dms:DeleteConnection"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:endpoint:*"
      ]
    },
    {
      "Sid" : "id4",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObjectTagging"
      ],
      "Resource" : [
        "arn:aws:s3:::dms-serverless-premigration-results-*",
        "arn:aws:s3:::dms-premigration-results-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "id5",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::dms-serverless-premigration-results-*",
        "arn:aws:s3:::dms-premigration-results-*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "id6",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTaskAssessmentRun"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:task:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSEC2CapacityManagerServiceRolePolicy

Descrição: permite que o EC2 Capacity Manager gerencie recursos de capacidade e se integre às AWS organizações em seu nome.

`AWSEC2CapacityManagerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Tempo de criação: 09 de outubro de 2025, 22:04 UTC
- Horário editado: 09 de outubro de 2025, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityManagerServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOrganizationsDefaultReadActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowOrganizationsListDelegatedAdministratorsAction",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "ec2.capacitymanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSEC2CapacityReservationFleetRolePolicy

Descrição: Permite que o serviço EC2 CapacityReservation Fleet gerencie reservas de capacidade

`AWSEC2CapacityReservationFleetRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 29 de setembro de 2021, 14:43 UTC

- Horário editado: 03 de março de 2025, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateCapacityReservation",
        "ec2:CancelCapacityReservation",
        "ec2:ModifyCapacityReservation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:CapacityReservationFleet" : "arn:aws:ec2:*:*:capacity-reservation-fleet/
crf-*"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateCapacityReservation"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSEC2FleetServiceRolePolicy

Descrição: permite que o EC2 Fleet inicie e gerencie instâncias.

`AWSEC2FleetServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 21 de março de 2018, 0:08 UTC
- Hora da edição: 04 de maio de 2020, 20:10 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2SpotManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2:fleet-id" : "*"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSEC2SpotFleetServiceRolePolicy

Descrição: permite que o EC2 Spot Fleet inicie e gerencie instâncias de frota spot.

`AWSEC2SpotFleetServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 23 de outubro de 2017, 19:13 UTC
- Hora da edição: 16 de março de 2020, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*",
        "arn:aws:ec2:*:*:spot-fleet-request/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:*/*"
      ]
    }
  ]
```

```
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSEC2SpotServiceRolePolicy

Descrição: permite que o EC2 Spot inicie e gerencie instâncias spot

`AWSEC2SpotServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 18 de setembro de 2017, 18:51 UTC
- Hora da edição: 12 de dezembro de 2018, 0:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "ec2:InstanceMarketType" : "spot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSEC2SqlHaInstancePolicy

Descrição: permissões de instância do Amazon EC2 para permitir que o serviço SQL High Availability do EC2 detecte o estado de alta disponibilidade da instância por meio do perfil de instância do EC2.

`AWSEC2SqlHaInstancePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSEC2SqlHaInstancePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 13 de novembro de 2025, 01:49 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2SqlHaInstancePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SqlHaMonitored" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSEc2SqlHa" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
```

```
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSEC2SqlHaServiceRolePolicy

Descrição: Permissões do serviço EC2 SQL High Availability para detectar instâncias standby/passive

`AWSEC2SqlHaServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 13 de novembro de 2025, 01:34 UTC
- Horário editado: 13 de novembro de 2025, 01:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SqlHaServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMSendCommandToTaggedInstances",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SqlHaMonitored" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSSMSendCommandOfOwnedDoc",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-DetectSqlHa*"
```

```
      ]
    },
    {
      "Sid" : "AllowSSMNonMutating",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2NonMutating",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEventsMutateManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ec2sqlha.amazonaws.com",
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      },
      "Resource" : "arn:aws:events:*:*:rule/AWSEC2SqlHa*"
    },
    {
      "Sid" : "AllowEventsNonMutatingManagedRule",
      "Effect" : "Allow",
```

```
      "Action" : [
        "events:ListTargetsByRule",
        "events:DescribeRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AWSEC2SqlHa*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSEC2VssRestorePolicy

Descrição: Concede permissões ao Amazon EC2 e ao AWS SSM para restaurar o banco de dados do SQL Server a partir de snapshots consistentes de aplicativos criados pelo VSS. AWS

`AWSEC2VssRestorePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSEC2VssRestorePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 25 de março de 2026, 23:12 UTC
- Horário editado: 25 de março de 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2VssRestorePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateVolumeAccessVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        },
        "ArnLike" : {
          "ec2:ParentSnapshot" : "arn:aws:ec2:*:*:snapshot/*"
        }
      }
    },
    {
      "Sid" : "CreateVolumeAccessSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/AwsVssConfig" : "*"
        }
      }
    },
    {
      "Sid" : "CreateVolumeWithTagging",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVolume"
        }
```

```
      }
    },
    {
      "Sid" : "AttachVolumeAccessVolume",
      "Effect" : "Allow",
      "Action" : "ec2:AttachVolume",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/AwsVssConfig" : "*"
        }
      }
    },
    {
      "Sid" : "AttachVolumeAccessInstance",
      "Effect" : "Allow",
      "Action" : "ec2:AttachVolume",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DescribeVolumes",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeVolumes",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeSnapshots",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSnapshots",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstanceAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstanceAttribute",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "SsmAutomationRead",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SsmRunCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AWSEC2-PrepareVssRestore",
        "arn:aws:ssm:*:*:document/AWSEC2-RunVssRestoreForSqlDatabase"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSEC2VssSnapshotPolicy

Descrição: esta política é anexada ao perfil do IAM associado a suas instâncias do Windows do Amazon EC2 para permitir que a solução VSS do Amazon EC2 crie e adicione tags a imagens de máquina da Amazon (AMI) e a snapshots do EBS.

`AWSEC2VssSnapshotPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSEC2VssSnapshotPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de março de 2024, 16:32 UTC
- Horário editado: 20 de novembro de 2024, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2VssSnapshotPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceInfo",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAccessInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAccessVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "CreateImageWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
```

```
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        }
      }
    },
    {
      "Sid" : "CreateImageAccessInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnResourceCreation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateImage",
            "CreateSnapshots"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsAfterResourceCreation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/AwsVssConfig" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AppConsistent",
            "Device"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeImagesAndSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSECRPullThroughCache_ServiceRolePolicy

Descrição: Permite o acesso a AWS serviços e recursos usados ou gerenciados pelo cache de extração do AWS ECR

`AWSECRPullThroughCache_ServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 26 de novembro de 2021, 21:51 UTC
- Horário editado: 12 de maio de 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECR",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage",
        "ecr:BatchGetImage",
```

```
        "ecr:BatchImportUpstreamImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetImageCopyStatus"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecr-pullthroughcache/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkCustomPlatformforEC2Role

Descrição: forneça permissão à instância em seu ambiente personalizado de criação de plataforma para iniciar a instância do EC2, criar snapshot e AMI do EBS, transmitir logs para o Amazon CloudWatch Logs e armazenar artefatos no Amazon S3.

`AWSElasticBeanstalkCustomPlatformforEC2Role` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticBeanstalkCustomPlatformforEC2Role` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 21 de fevereiro de 2017, 22:50 UTC
- Hora da edição: 21 de fevereiro de 2017, 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Access",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateKeypair",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteKeypair",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSnapshot",
```

```
        "ec2:DeleteVolume",
        "ec2:DeregisterImage",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "ec2:GetPasswordData",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySnapshotAttribute",
        "ec2:RegisterImage",
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/platform/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkEKSImageBuild

Descrição: Permissões necessárias ao Elastic Beanstalk para criar imagens de contêiner em nome do cliente.

`AWSElasticBeanstalkEKSImageBuild` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticBeanstalkEKSImageBuild` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 02 de julho de 2026, 21:27 UTC
- Horário editado: 02 de julho de 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkEKSImageBuild`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3SourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ECRAuthToken",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ECRPublicAuthToken",
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
```

```
        "sts:GetServiceBearerToken"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ECRRepositoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:PutImage",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkEKSObservability

Descrição: Permissões de observabilidade para ambientes do Elastic Beanstalk em execução no cluster do Elastic Kubernetes Service

`AWSElasticBeanstalkEKSObservability` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticBeanstalkEKSObservability` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 02 de julho de 2026, 21:27 UTC
- Horário editado: 02 de julho de 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkEKSObservability`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FluentBitS3Plugin",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-logs-*",
        "arn:aws:s3:::elasticbeanstalk-logs-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "APSCreateWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace",
        "aps:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "ElasticBeanstalk",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "APSManageWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aps:DeleteWorkspace",
```

```
        "aps:Describe*"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "ElasticBeanstalk",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "APSRemoteWrite",
      "Effect" : "Allow",
      "Action" : [
        "aps:RemoteWrite"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "ElasticBeanstalk",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkEKSTagging

Descrição: Permissões necessárias para passar por tags para recursos criados pelos controladores EKS

`AWSElasticBeanstalkEKSTagging` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticBeanstalkEKSTagging` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 02 de julho de 2026, 21:27 UTC
- Horário editado: 02 de julho de 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkEKSTagging`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Compute",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-node-class-name" : "*",
```

```
          "aws:RequestTag/eks:kubernetes-node-pool-name" : "*"
        }
      }
    },
    {
      "Sid" : "Storage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Sid" : "Networking",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-cni-node-name" : "*"
        }
      }
    },
    {
      "Sid" : "LoadBalancer",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:CreateListener",
```

```
        "elasticloadbalancing:CreateRule",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Sid" : "ShieldProtection",
      "Effect" : "Allow",
      "Action" : [
        "shield:CreateProtection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Sid" : "ShieldTagResource",
      "Effect" : "Allow",
      "Action" : [
        "shield:TagResource"
      ],
      "Resource" : "arn:aws:shield::*:protection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkEnhancedHealth

Descrição: Política do AWS Elastic Beanstalk Service para sistema de monitoramento de saúde

`AWSElasticBeanstalkEnhancedHealth` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticBeanstalkEnhancedHealth` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 08 de fevereiro de 2016, 23:17 UTC
- Hora da edição: 09 de abril de 2018, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:GetConsoleOutput",
        "ec2:AssociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeSecurityGroups",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeNotificationConfigurations",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*:log-stream:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkMaintenance

Descrição: Política de função de serviço do AWS Elastic Beanstalk que concede permissões limitadas para atualizar seus recursos em seu nome para fins de manutenção.

`AWSElasticBeanstalkMaintenance` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 11 de janeiro de 2019, 23:22 UTC
- Hora da edição: 29 de abril de 2024, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "AllowCloudformationChangeSetOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStacks",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowElasticBeanstalkStacksUpdateExecuteSuccessfully",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

Descrição: Essa política é para a função de serviço do AWS Elastic Beanstalk usada para realizar atualizações gerenciadas dos ambientes do Elastic Beanstalk. Essa política não deve ser vinculada a outros usuários ou funções. A política concede amplas permissões para criar e gerenciar recursos em vários AWS serviços AutoScaling, incluindo EC2, ECS, Elastic Load Balancing e. CloudFormation Essa política também permite a transmissão de qualquer função do IAM utilizável com esses serviços.

`AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 03 de março de 2021, 22:18 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticBeanstalkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeInstanceHealth",
```

```
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "logs:DescribeLogGroups",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2BroadOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteSecurityGroup",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2RunInstancesOperationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
```

```
    },
    {
      "Sid" : "EC2TerminateInstancesOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Sid" : "ECSBroadOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:DescribeClusters",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECSDeleteClusterOperationPermissions",
      "Effect" : "Allow",
      "Action" : "ecs:DeleteCluster",
      "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
    },
    {
      "Sid" : "ASGOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteScheduledAction",
```

```
        "autoscaling:DetachInstances",
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:ResumeProcesses",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Sid" : "CFNOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "ELBOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
```

```
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/*"
      ]
    },
    {
      "Sid" : "CWLogsOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "S3ObjectOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Sid" : "S3BucketOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
```

```
    },
    {
      "Sid" : "SNSOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Subscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
    },
    {
      "Sid" : "SQSOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:awseb-e-*",
        "arn:aws:sqs:*:*:eb-*"
      ]
    },
    {
      "Sid" : "CWPutMetricAlarmOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:awseb-*",
        "arn:aws:cloudwatch:*:*:alarm:eb-*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchTemplateTagPropagationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:createTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "RunInstances",
            "AllocateAddress"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

Descrição: Política de função de serviço do AWS Elastic Beanstalk que concede permissões limitadas às atualizações gerenciadas.

`AWSElasticBeanstalkManagedUpdatesServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 21 de novembro de 2019, 22:35 UTC
- Horário editado: 13 de março de 2026, 16:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
```

```
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SingleInstanceAPIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:releaseAddress",
        "ec2:allocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterTaskDefinition",
        "ecs:DeRegisterTaskDefinition",
        "ecs:List*",
        "ecs:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElasticBeanstalkAPIs",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyAPIs",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:List*",
        "ec2:Describe*",
        "autoscaling:Describe*",
        "elasticloadbalancing:Describe*",
```

```
        "logs:DescribeLogGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Sid" : "CFN",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CancelUpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
```

```
        "cloudformation:UpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-e-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Sid" : "S3Obj",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Sid" : "S3Bucket",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "CWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "ELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-e-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*"
      ]
    },
    {
      "Sid" : "SNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-Environment-*"
    },
    {
      "Sid" : "EC2LaunchTemplate",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*"
    },
    {
      "Sid" : "AllowLaunchTemplateRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RegisterTaskDefinition"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchTemplateTagPropagationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:createTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "RunInstances",
```

```
            "AllocateAddress"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkMulticontainerDocker

Descrição: fornece às instâncias em seu ambiente de vários contêineres do Docker acesso para usar o Amazon EC2 Container Service para gerenciar tarefas de implantação de contêineres.

`AWSElasticBeanstalkMulticontainerDocker` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticBeanstalkMulticontainerDocker` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de fevereiro de 2016, 23:15 UTC
- Horário editado: 29 de abril de 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecs:Poll",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:DiscoverPollEndpoint",
        "ecs:StartTelemetrySession",
        "ecs:RegisterContainerInstance",
        "ecs:DeregisterContainerInstance",
        "ecs:DescribeContainerInstances",
        "ecs:Submit*",
        "ecs:DescribeTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RegisterContainerInstance",
            "StartTask"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "AIEnvironmentAnalysisInvokeFoundationModel",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/anthropic.claude-*",
        "arn:aws:bedrock:*::foundation-model/amazon.nova-*"
      ]
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeInferenceProfile",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*anthropic.claude-*",
        "arn:aws:bedrock:*:*:inference-profile/*amazon.nova-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AIEnvironmentAnalysisReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels",
        "elasticbeanstalk:DescribeEvents",
        "elasticbeanstalk:DescribeEnvironmentHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrock",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkReadOnly

Descrição: concede permissões somente leitura. Permite explicitamente que os operadores obtenham acesso direto para recuperar informações sobre recursos relacionados aos aplicativos do AWS Elastic Beanstalk.

`AWSElasticBeanstalkReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticBeanstalkReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 22 de janeiro de 2021, 19:02 UTC
- Horário editado: 19 de maio de 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAPIs",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ValidateTemplate",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeAvailabilityZones",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribeDBSnapshots",
        "s3:ListAllMyBuckets",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
```

```
      "Sid" : "AllowCloudWatchLogsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "AllowCloudWatchLogsRead",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*:log-stream:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkRoleCore

Descrição: AWSElasticBeanstalkRoleCore (função de operações do Elastic Beanstalk) Permite a operação central de um ambiente de serviço web.

`AWSElasticBeanstalkRoleCore` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticBeanstalkRoleCore` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço

- Hora da criação: 05 de junho de 2020, 21:48 UTC
- Hora da edição: 30 de abril de 2024, 0:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/awseb-e-*"
        }
      }
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReleaseAddress",
        "ec2:AllocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress",
        "ec2:CreateTags",
        "ec2:DeleteTags",
```

```
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroup*",
        "ec2:RevokeSecurityGroup*",
        "ec2:CreateLaunchTemplate*",
        "ec2:DeleteLaunchTemplate*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LTRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:*LoadBalancer*",
        "autoscaling:*AutoScalingGroup",
        "autoscaling:*LaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:*Tags"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*"
      ]
    },
    {
```

```
      "Sid" : "ASGPolicy",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EBSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticbeanstalk.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Obj",
      "Effect" : "Allow",
      "Action" : [
        "s3:Delete*",
        "s3:Get*",
        "s3:Put*"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*/*",
        "arn:aws:s3:::elasticbeanstalk-env-resources-*/*"
      ]
    },
    {
      "Sid" : "S3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucket*",
        "s3:ListBucket",
```

```
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "CFN",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:UpdateStack",
        "cloudformation:ContinueUpdateRollback",
        "cloudformation:CancelUpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/awseb-e-*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:awseb-*"
    },
    {
      "Sid" : "ELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Create*",
        "elasticloadbalancing:Delete*",
        "elasticloadbalancing:Modify*",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:*Tags",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:SetRulePriorities",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
```

```
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/net/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/*/*/*"
      ]
    },
    {
      "Sid" : "ListAPIs",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "logs:Describe*",
        "ec2:Describe*",
        "ecs:Describe*",
        "ecs:List*",
        "elasticloadbalancing:Describe*",
        "rds:Describe*",
        "sns:List*",
        "iam:List*",
        "acm:Describe*",
        "acm:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
```

```
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkRoleCWL

Descrição: (função de operações do Elastic Beanstalk) Permite que um ambiente gerencie grupos de CloudWatch logs do Amazon Logs.

`AWSElasticBeanstalkRoleCWL` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticBeanstalkRoleCWL` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 05 de junho de 2020, 21:49 UTC
- Hora da edição: 05 de junho de 2020, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkRoleECS

Descrição: (perfil de operações do Elastic Beanstalk) Permite que um ambiente de vários contêineres do Docker gerencie clusters do Amazon ECS.

`AWSElasticBeanstalkRoleECS` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticBeanstalkRoleECS` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 05 de junho de 2020, 21:47 UTC
- Hora da edição: 23 de março de 2023, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:RegisterTaskDefinition",
        "ecs:DeRegisterTaskDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkRoleRDS

Descrição: (perfil de operações do Elastic Beanstalk) Permite que um ambiente integre uma instância do Amazon RDS.

`AWSElasticBeanstalkRoleRDS` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticBeanstalkRoleRDS` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 05 de junho de 2020, 21:46 UTC
- Hora da edição: 05 de junho de 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBSecurityGroup",
        "rds:DeleteDBSecurityGroup",
        "rds:AuthorizeDBSecurityGroupIngress",
        "rds:CreateDBInstance",
        "rds:ModifyDBInstance",
        "rds:DeleteDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:secgrp:awseb-e-*",
        "arn:aws:rds:*:*:db:*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkRoleSNS

Descrição: (perfil de operações do Elastic Beanstalk) Permite que um ambiente habilite a integração de tópicos do Amazon SNS.

`AWSElasticBeanstalkRoleSNS` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticBeanstalkRoleSNS` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 05 de junho de 2020, 21:46 UTC
- Hora da edição: 05 de junho de 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowBeanstalkManageSNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns:DeleteTopic"
      ],
```

```
      "Resource" : [
        "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
      ]
    },
    {
      "Sid" : "AllowSNSPublish",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkRoleWorkerTier

Descrição: (perfil de operações do Elastic Beanstalk) permite que um nível de ambiente de operador crie uma tabela do Amazon DynamoDB e uma fila do Amazon SQS.

`AWSElasticBeanstalkRoleWorkerTier` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticBeanstalkRoleWorkerTier` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço

- Hora da criação: 05 de junho de 2020, 21:43 UTC
- Hora da edição: 05 de junho de 2020, 21:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSQS",
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:CreateQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:awseb-e-*"
    },
    {
      "Sid" : "AllowDDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:TagResource",
        "dynamodb:DescribeTable",
        "dynamodb:DeleteTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/awseb-e-*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkService

Descrição: esta política será descontinuada. Consulte a documentação para obter orientação: Política de função do https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html. AWS Elastic Beanstalk Service que concede permissões para criar e gerenciar recursos (por exemplo: AutoScaling EC2, S3 CloudFormation, ELB etc.) em seu nome.

`AWSElasticBeanstalkService` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticBeanstalkService` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 11 de abril de 2016, 20:27 UTC
- Hora da edição: 10 de maio de 2023, 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

Versão da política

Versão da política: v17 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowDeleteCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "AllowS3OperationsOnElasticBeanstalkBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:*"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "AllowLaunchTemplateRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "AllowELBAddTags",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOperations",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
```

```
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DetachInstances",
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:ResumeProcesses",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
        "cloudwatch:PutMetricAlarm",
        "ec2:AssociateAddress",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceAttribute",
```

```
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeVpcClassicLink",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:TerminateInstances",
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:DescribeClusters",
        "ecs:RegisterTaskDefinition",
        "elasticbeanstalk:*",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "iam:ListRoles",
        "iam:PassRole",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogGroups",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:ListBucket",
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:Subscribe",
        "sns:SetTopicAttributes",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
```

```
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkServiceRolePolicy

Descrição: Política de função vinculada do AWS Elastic Beanstalk Service, que concede permissões para criar e gerenciar recursos (ou seja AutoScaling, EC2, S3 CloudFormation, ELB etc.) em seu nome.

`AWSElasticBeanstalkServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 13 de setembro de 2017, 23:46 UTC
- Horário editado: 18 de agosto de 2026, 17:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationReadOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowOperations",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:PutNotificationConfiguration",
        "ec2:DescribeInstanceStatus",
        "ec2:AssociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
```

```
        "elasticloadbalancing:DescribeTargetGroups",
        "lambda:GetFunction",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOperationsOnHealthStreamingLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DeleteLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "EBEKSGeneralOperations",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:DescribeRepositories",
        "ecr:ListTagsForResource",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
```

```
        "iam:GetRole",
        "codebuild:ListProjects",
        "codebuild:BatchGetProjects",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "elasticbeanstalk:DescribeEvents",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticbeanstalk:DescribeConfigurationSettings"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSDefaultHTTPSCertCreate",
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSDefaultHTTPSCertModifyDelete",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:DeleteCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:environment-id" : "false"
```

```
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSSubnetTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "kubernetes.io/role/elb",
            "kubernetes.io/role/internal-elb"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSIamCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:AWSServiceName" : "eks.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EBEKSIamPermissionsImageBuild",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "codebuild.amazonaws.com",
            "eks.amazonaws.com",
            "ec2.amazonaws.com",
            "pods.eks.amazonaws.com",
            "elasticbeanstalk.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EBEKSS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetObjectVersion",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSEKSClusterManagement",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateCluster",
        "eks:DeleteCluster",
        "eks:DescribeCluster",
        "eks:DescribeUpdate",
```

```
        "eks:CreateAccessEntry",
        "eks:DeleteAccessEntry",
        "eks:CreateAddon",
        "eks:CreatePodIdentityAssociation",
        "eks:ListPodIdentityAssociations"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/beanstalk-cluster*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSEKSAddonManagement",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeleteAddon",
        "eks:DescribeAddon",
        "eks:UpdateAddon"
      ],
      "Resource" : "arn:aws:eks:*:*:addon/beanstalk-cluster*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSEKSAccessEntryManagement",
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/beanstalk-cluster*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "EBEKSEKSPodIdentityManagement",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeletePodIdentityAssociation",
        "eks:DescribePodIdentityAssociation",
        "eks:UpdatePodIdentityAssociation"
      ],
      "Resource" : "arn:aws:eks:*:*:podidentityassociation/beanstalk-cluster*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSCodeBuildProjectManagement",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:UpdateProject",
        "codebuild:StartBuild",
        "codebuild:BatchGetBuilds",
        "codebuild:BatchGetProjects"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSECRRepositoryManagement",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:DescribeRepositories",
        "ecr:DescribeImages",
        "ecr:PutLifecyclePolicy",
        "ecr:TagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSCFNStackManagementImageBuild",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/elasticbeanstalk-*-image-build",
        "arn:aws:cloudformation:*:*:stack/elasticbeanstalk-*-image-build/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSCFNStackManagementClusterSetup",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/beanstalk-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "EBEKSAPSCreateWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace",
        "aps:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "ElasticBeanstalk",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSAPSManageWorkspace",
      "Effect" : "Allow",
      "Action" : [
        "aps:DeleteWorkspace",
        "aps:Describe*"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "ElasticBeanstalk"
        }
      }
    },
    {
      "Sid" : "EBEKSAPSRemoteWrite",
      "Effect" : "Allow",
      "Action" : [
        "aps:RemoteWrite"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "ElasticBeanstalk"
        }
      }
    },
    {
```

```
      "Sid" : "EBEKSCreateDashboard",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutDashboard",
      "Resource" : "arn:aws:cloudwatch::*:dashboard/ElasticBeanstalk-Observability-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbLoadBalancerWrite",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:SetSecurityGroups",
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbTargetGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbTargetGroupModifyDelete",
      "Effect" : "Allow",
```

```
      "Action" : [
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbListenerRuleCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbListenerRuleDelete",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteRule"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbEC2CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/elasticbeanstalk:byo-alb-arn" : "false",
          "aws:RequestTag/elasticbeanstalk:managed" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbEC2CreateSecurityGroupVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbEC2CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
```

```
      "Condition" : {
        "Null" : {
          "aws:RequestTag/elasticbeanstalk:byo-alb-arn" : "false",
          "aws:RequestTag/elasticbeanstalk:managed" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "EBEKSByoAlbEC2SecurityGroupEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:byo-alb-arn" : "false",
          "aws:ResourceTag/elasticbeanstalk:managed" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ECRTagMutation",
      "Effect" : "Allow",
      "Action" : [
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:application-name" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "CodeBuildTagMutation",
      "Effect" : "Allow",
      "Action" : "codebuild:UpdateProject",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:application-name" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagMutation",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:RemoveTagsFromCertificate",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:RemoveTags",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/elasticbeanstalk:environment-id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkWebTier

Descrição: fornece às instâncias em seu ambiente de servidor Web acesso para fazer upload de arquivos de log para o Amazon S3.

`AWSElasticBeanstalkWebTier` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticBeanstalkWebTier` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de fevereiro de 2016, 23:08 UTC
- Horário editado: 29 de abril de 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
```

```
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "XRayAccess",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "ElasticBeanstalkHealthAccess",
      "Action" : [
        "elasticbeanstalk:PutInstanceStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:elasticbeanstalk:*:*:application/*",
        "arn:aws:elasticbeanstalk:*:*:environment/*"
      ]
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeFoundationModel",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
```

```
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/anthropic.claude-*",
        "arn:aws:bedrock:*::foundation-model/amazon.nova-*"
      ]
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeInferenceProfile",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*anthropic.claude-*",
        "arn:aws:bedrock:*:*:inference-profile/*amazon.nova-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AIEnvironmentAnalysisReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels",
        "elasticbeanstalk:DescribeEvents",
        "elasticbeanstalk:DescribeEnvironmentHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrock",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticBeanstalkWorkerTier

Descrição: forneça às instâncias em seu ambiente de trabalho acesso para fazer upload de arquivos de log para o Amazon S3, usar o Amazon SQS para monitorar a fila de trabalhos do seu aplicativo, usar o Amazon DynamoDB para realizar a eleição de líderes e para a Amazon publicar métricas para monitoramento da CloudWatch saúde.

`AWSElasticBeanstalkWorkerTier` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticBeanstalkWorkerTier` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de fevereiro de 2016, 23:12 UTC
- Horário editado: 29 de abril de 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MetricsAccess",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "XRayAccess",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "QueueAccess",
      "Action" : [
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "DynamoPeriodicTasks",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DeleteItem",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:UpdateItem"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/*-stack-AWSEBWorkerCronLeaderRegistry*"
      ]
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "ElasticBeanstalkHealthAccess",
      "Action" : [
        "elasticbeanstalk:PutInstanceStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:elasticbeanstalk:*:*:application/*",
        "arn:aws:elasticbeanstalk:*:*:environment/*"
      ]
```

```
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeFoundationModel",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/anthropic.claude-*",
        "arn:aws:bedrock:*::foundation-model/amazon.nova-*"
      ]
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeInferenceProfile",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*anthropic.claude-*",
        "arn:aws:bedrock:*:*:inference-profile/*amazon.nova-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AIEnvironmentAnalysisReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels",
        "elasticbeanstalk:DescribeEvents",
        "elasticbeanstalk:DescribeEnvironmentHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrock",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticDisasterRecoveryAgentInstallationPolicy

Descrição: Essa política permite instalar o Agente de AWS Replicação, que é usado com o AWS Elastic Disaster Recovery (DRS) para recuperar servidores externos em. AWS Anexe essa política aos seus usuários ou funções do IAM cujas credenciais você fornece durante a etapa de instalação do Agente de AWS Replicação.

`AWSElasticDisasterRecoveryAgentInstallationPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryAgentInstallationPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de novembro de 2021, 10:37 UTC
- Hora da edição: 27 de novembro de 2023, 12:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentInstallationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateRecoveryInstanceForDrs",
        "drs:DescribeRecoveryInstances",
        "drs:CreateSourceNetwork"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSAgentInstallationPolicy2",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy3",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateRecoveryInstanceForDrs"
        }
```

```
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy4",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-network/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceNetwork"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy5",
      "Effect" : "Allow",
      "Action" : "drs:IssueAgentCertificateForDrs",
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticDisasterRecoveryAgentPolicy

Descrição: Essa política permite usar o Agente de AWS Replicação, que é usado com o AWS Elastic Disaster Recovery (DRS) para recuperar servidores de origem em. AWS Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM.

`AWSElasticDisasterRecoveryAgentPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryAgentPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 17 de novembro de 2021, 10:32 UTC
- Hora da edição: 27 de novembro de 2023, 13:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
```

```
        "drs:IssueAgentCertificateForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/${aws:SourceIdentity}"
    },
    {
      "Sid" : "DRSAgentPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticDisasterRecoveryConsoleFullAccess

Descrição: Essa política fornece acesso total a todas as APIs públicas do AWS Elastic Disaster Recovery (DRS), bem como permissões para ler informações da chave KMS, do License Manager, dos grupos de recursos, do Elastic Load Balancing, do IAM e do EC2. Anexe essa política aos seus usuários ou funções do IAM.

`AWSElasticDisasterRecoveryConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 17 de novembro de 2021, 10:46 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
```

```
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess4",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess5",
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess6",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess7",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess8",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
```

```
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess16",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "ConsoleFullAccess17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess19",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:StartInstances",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
```

```
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
```

```
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess25",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
```

```
            "CreateSnapshot",
            "RunInstances"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess28",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess29",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess30",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticDisasterRecoveryConsoleFullAccess_v2

Descrição: Essa política fornece acesso total a todas as APIs públicas do AWS Elastic Disaster Recovery (AWS DRS), bem como a todas as APIs públicas em outros AWS serviços usados pelo AWS DRS Console. Anexe essa política aos seus usuários ou perfis.

`AWSElasticDisasterRecoveryConsoleFullAccess_v2` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryConsoleFullAccess_v2` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de novembro de 2023, 13:35 UTC

- Horário editado: 18 de junho de 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
```

```
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts",
        "ec2:GetInstanceTypesFromInstanceRequirements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess4",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess5",
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess6",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess7",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess8",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
```

```
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
```

```
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
```

```
      },
      "Null" : {
        "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess16",
    "Effect" : "Allow",
    "Action" : "ec2:CreateSecurityGroup",
    "Resource" : "arn:aws:ec2:*:*:vpc/*"
  },
  {
    "Sid" : "ConsoleFullAccess17",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup"
    ],
    "Resource" : "arn:aws:ec2:*:*:security-group/*",
    "Condition" : {
      "Bool" : {
        "aws:ViaAWSService" : "true"
      },
      "Null" : {
        "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess18",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "Bool" : {
        "aws:ViaAWSService" : "true"
      },
      "Null" : {
        "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
```

```
    {
      "Sid" : "ConsoleFullAccess19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:StartInstances",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess24",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess25",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
```

```
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess28",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess29",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "ConsoleFullAccess30",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess31",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-CreateImage:$DEFAULT",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSDRS-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSDRS-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSDRS-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSDRS-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSDRS-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSDRS-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSDRS-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSDRS-VerifyTags",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure",
```

```
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess32",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess33",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess34",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
```

```
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess35",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ConsoleFullAccess36",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess37",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess38",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess39",
      "Effect" : "Allow",
      "Action" : "ec2:CreateFleet",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess40",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess41",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess42",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
```

```
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess43",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "ConsoleFullAccess44",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticDisasterRecoveryConversionServerPolicy

Descrição: Essa política está anexada à função de instância do servidor AWS Elastic Disaster Recovery Conversion. Essa política permite que os servidores de conversão do Elastic Disaster Recovery (DRS), que são instâncias EC2 lançadas pelo Elastic Disaster Recovery, se comuniquem com o serviço DRS. Uma função do IAM com essa política é anexada (como um perfil de instância do EC2) pelo DRS aos servidores de conversão do DRS, que são iniciados e encerrados automaticamente pelo DRS, quando necessário. Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM. Os servidores de conversão DRS são usados pelo Elastic Disaster Recovery quando os usuários optam por recuperar servidores de origem usando o console, a CLI ou a API do DRS.

`AWSElasticDisasterRecoveryConversionServerPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryConversionServerPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 17 de novembro de 2021, 13:42 UTC
- Hora da edição: 27 de novembro de 2023, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSConversionServerPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSConversionServerPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

Descrição: Essa política permite que o AWS Elastic Disaster Recovery (DRS) ofereça suporte à replicação entre contas e ao failback entre contas.

`AWSElasticDisasterRecoveryCrossAccountReplicationPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryCrossAccountReplicationPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 14 de maio de 2023, 7:16 UTC
- Hora da edição: 17 de janeiro de 2024, 13:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CrossAccountPolicy1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeInstances",
        "drs:DescribeSourceServers",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:CreateSourceServerForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccountPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticDisasterRecoveryEc2InstancePolicy

Descrição: Essa política permite instalar e usar o Agente de AWS Replicação, que é usado pelo AWS Elastic Disaster Recovery (DRS) para recuperar servidores de origem executados no EC2 (entre regiões ou cross-AZ). Uma função do IAM com essa política deve ser anexada (como um perfil de instância do EC2) às instâncias do EC2.

`AWSElasticDisasterRecoveryEc2InstancePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryEc2InstancePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 26 de maio de 2022, 12:30 UTC
- Hora da edição: 27 de novembro de 2023, 13:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSEc2InstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateSourceNetwork"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSEc2InstancePolicy2",
```

```
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSEc2InstancePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-network/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceNetwork"
        }
      }
    },
    {
      "Sid" : "DRSEc2InstancePolicy4",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSEc2InstancePolicy5",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/DRSCrossAccountAgentAuthorizedRole_*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SourceInstanceARN" : "${ec2:SourceInstanceARN}"
        },
        "ForAnyValue:StringEquals" : {
          "sts:TransitiveTagKeys" : "SourceInstanceARN"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticDisasterRecoveryFailbackInstallationPolicy

Descrição: você pode anexar a AWSElasticDisasterRecoveryFailbackInstallationPolicy política às suas identidades do IAM. Essa política permite instalar o Elastic Disaster Recovery Failback Client, que é usado para retornar instâncias de recuperação à sua infraestrutura de origem. Anexe essa política aos seus usuários ou perfis do IAM cujas credenciais você fornece ao executar o Elastic Disaster Recovery Failback Client.

`AWSElasticDisasterRecoveryFailbackInstallationPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryFailbackInstallationPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de novembro de 2021, 11:02 UTC
- Hora da edição: 27 de novembro de 2023, 13:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSFailbackInstallationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "DRSFailbackInstallationPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource",
        "drs:IssueAgentCertificateForDrs",
        "drs:AssociateFailbackClientToRecoveryInstanceForDrs",
        "drs:GetSuggestedFailbackClientDeviceMappingForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateFailbackClientDeviceMappingForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticDisasterRecoveryFailbackPolicy

Descrição: esta política permite usar o Elastic Disaster Recovery Failback Client, que é usado para retornar instâncias de recuperação à sua infraestrutura de origem original. Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM.

`AWSElasticDisasterRecoveryFailbackPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryFailbackPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço

- Hora da criação: 17 de novembro de 2021, 10:41 UTC
- Horário editado: 22 de julho de 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSFailbackPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeReplicationServerAssociationsForDrs",
```

```
        "drs:DescribeRecoveryInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetFailbackCommandForDrs",
        "drs:UpdateFailbackClientLastSeenForDrs",
        "drs:NotifyAgentAuthenticationForDrs",
        "drs:UpdateAgentReplicationProcessStateForDrs",
        "drs:NotifyAgentReplicationProgressForDrs",
        "drs:NotifyAgentConnectedForDrs",
        "drs:NotifyAgentDisconnectedForDrs",
        "drs:NotifyConsistencyAttainedForDrs",
        "drs:GetFailbackLaunchRequestedForDrs",
        "drs:IssueAgentCertificateForDrs",
        "drs:GetAgentSnapshotCreditsForDrs",
        "drs:SendVolumeStatsForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/${aws:SourceIdentity}"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticDisasterRecoveryLaunchActionsPolicy

Descrição: Essa política permite que você use as permissões necessárias do Amazon SSM e de serviços adicionais para executar ações pós-lançamento no AWS Elastic Disaster Recovery (DRS).AWS Anexe essa política aos seus perfis ou usuários do IAM.

`AWSElasticDisasterRecoveryLaunchActionsPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryLaunchActionsPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 13 de setembro de 2023, 7:38 UTC
- Horário editado: 18 de junho de 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LaunchActionsPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-definition/*:*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-*",
        "arn:aws:ssm:*::document/AWSCodeDeployAgent-*",
        "arn:aws:ssm:*::document/AWSConfigRemediation-*",
        "arn:aws:ssm:*::document/AWSConformancePacks-*",
        "arn:aws:ssm:*::document/AWSDisasterRecovery-*",
        "arn:aws:ssm:*::document/AWSDistroOTel-*",
        "arn:aws:ssm:*::document/AWSDocs-*",
        "arn:aws:ssm:*::document/AWSDRS-*",
        "arn:aws:ssm:*::document/AWSEC2-*",
```

```
        "arn:aws:ssm:*::document/AWSEC2Launch-*",
        "arn:aws:ssm:*::document/AWSFIS-*",
        "arn:aws:ssm:*::document/AWSFleetManager-*",
        "arn:aws:ssm:*::document/AWSIncidents-*",
        "arn:aws:ssm:*::document/AWSKinesisTap-*",
        "arn:aws:ssm:*::document/AWSMigration-*",
        "arn:aws:ssm:*::document/AWSNVMe-*",
        "arn:aws:ssm:*::document/AWSNitroEnclavesWindows-*",
        "arn:aws:ssm:*::document/AWSObservabilityExporter-*",
        "arn:aws:ssm:*::document/AWSPVDriver-*",
        "arn:aws:ssm:*::document/AWSQuickSetupType-*",
        "arn:aws:ssm:*::document/AWSQuickStarts-*",
        "arn:aws:ssm:*::document/AWSRefactorSpaces-*",
        "arn:aws:ssm:*::document/AWSResilienceHub-*",
        "arn:aws:ssm:*::document/AWSSAP-*",
        "arn:aws:ssm:*::document/AWSSAPTools-*",
        "arn:aws:ssm:*::document/AWSSQLServer-*",
        "arn:aws:ssm:*::document/AWSSSO-*",
        "arn:aws:ssm:*::document/AWSSupport-*",
        "arn:aws:ssm:*::document/AWSSystemsManagerSAP-*",
        "arn:aws:ssm:*::document/AmazonCloudWatch-*",
        "arn:aws:ssm:*::document/AmazonCloudWatchAgent-*",
        "arn:aws:ssm:*::document/AmazonECS-*",
        "arn:aws:ssm:*::document/AmazonEFSUtils-*",
        "arn:aws:ssm:*::document/AmazonEKS-*",
        "arn:aws:ssm:*::document/AmazonInspector-*",
        "arn:aws:ssm:*::document/AmazonInspector2-*",
        "arn:aws:ssm:*::document/AmazonInternal-*",
        "arn:aws:ssm:*::document/AwsEnaNetworkDriver-*",
        "arn:aws:ssm:*::document/AwsVssComponents-*",
        "arn:aws:ssm:*::automation-definition/AWS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSCodeDeployAgent-*:*",
        "arn:aws:ssm:*::automation-definition/AWSConfigRemediation-*:*",
        "arn:aws:ssm:*::automation-definition/AWSConformancePacks-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDisasterRecovery-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDistroOTel-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDocs-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDRS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2Launch-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFIS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFleetManager-*:*",
        "arn:aws:ssm:*::automation-definition/AWSIncidents-*:*",
        "arn:aws:ssm:*::automation-definition/AWSKinesisTap-*:*",
```

```
        "arn:aws:ssm:*::automation-definition/AWSMigration-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNVMe-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNitroEnclavesWindows-*:*",
        "arn:aws:ssm:*::automation-definition/AWSObservabilityExporter-*:*",
        "arn:aws:ssm:*::automation-definition/AWSPVDriver-*:*",
        "arn:aws:ssm:*::automation-definition/AWSQuickSetupType-*:*",
        "arn:aws:ssm:*::automation-definition/AWSQuickStarts-*:*",
        "arn:aws:ssm:*::automation-definition/AWSRefactorSpaces-*:*",
        "arn:aws:ssm:*::automation-definition/AWSResilienceHub-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAPTools-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSQLServer-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSSO-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSupport-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSystemsManagerSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatch-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatchAgent-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonECS-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEFSUtils-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEKS-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInspector-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInspector2-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInternal-*:*",
        "arn:aws:ssm:*::automation-definition/AwsEnaNetworkDriver-*:*",
        "arn:aws:ssm:*::automation-definition/AwsVssComponents-*:*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LaunchActionsPolicy7",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:ListDocumentVersions",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "LaunchActionsPolicy8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy9",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy10",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy11",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "drs.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticDisasterRecoveryNetworkReplicationPolicy

Descrição: Essa política permite que o AWS Elastic Disaster Recovery (DRS) ofereça suporte à replicação de rede.

`AWSElasticDisasterRecoveryNetworkReplicationPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryNetworkReplicationPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 11 de junho de 2023, 12:36 UTC
- Hora da edição: 2 de janeiro de 2024, 13:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSNetworkReplicationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
```

```
        "ec2:DescribeInstances",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedPrefixListAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticDisasterRecoveryReadOnlyAccess

Descrição: você pode anexar a AWSElasticDisasterRecoveryReadOnlyAccess política às suas identidades do IAM. Essa política fornece permissões para todas as APIs públicas somente para leitura do Elastic Disaster Recovery (DRS), bem como para algumas APIs somente para leitura de outros AWS serviços que são necessárias para fazer uso completo do console DRS somente para leitura. Anexe essa política aos seus usuários ou funções do IAM.

`AWSElasticDisasterRecoveryReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de novembro de 2021, 10:50 UTC
- Horário editado: 18 de agosto de 2026, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReadOnlyAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "drs:ListLaunchActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:GetInstanceTypesFromInstanceRequirements"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess4",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess5",
      "Effect" : "Allow",
      "Action" : "ssm:ListCommandInvocations",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess6",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameter",
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
    },
    {
      "Sid" : "DRSReadOnlyAccess7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-CreateImage",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure"
      ]
    },
    {
      "Sid" : "DRSReadOnlyAccess8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
```

```
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSReadOnlyAccess9",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetRecoveryPlan",
        "drs:ListRecoveryPlans",
        "drs:GetRecoveryPlanStep",
        "drs:ListRecoveryPlanSteps",
        "drs:GetRecoveryPlanExecution",
        "drs:ListRecoveryPlanExecutions",
        "drs:GetRecoveryPlanExecutionStep",
        "drs:ListRecoveryPlanExecutionSteps"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticDisasterRecoveryRecoveryInstancePolicy

Descrição: esta política está vinculada ao perfil de instância da Instância de Recuperação do Elastic Disaster Recovery. Essa política permite que a Instância de Recuperação do Elastic Disaster Recovery (DRS), que são instâncias do EC2 lançadas pela Elastic Disaster Recovery, se comunique com o serviço DRS e seja capaz de dar failback à sua infraestrutura de origem. Uma função do IAM com essa política é anexada (como um perfil de instância do EC2) pela Elastic Disaster Recovery

às instâncias de recuperação do DRS. Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM.

`AWSElasticDisasterRecoveryRecoveryInstancePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryRecoveryInstancePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 17 de novembro de 2021, 10:20 UTC
- Hora da edição: 27 de novembro de 2023, 13:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSRecoveryInstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
```

```
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
        "drs:UpdateReplicationCertificateForDrs",
        "drs:NotifyReplicationServerAuthenticationForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*",
      "Condition" : {
        "StringEquals" : {
          "drs:EC2InstanceARN" : "${ec2:SourceInstanceARN}"
        }
      }
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeRecoveryInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy4",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:CreateSourceServerForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy5",
```

```
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy6",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy7",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/DRSCrossAccountAgentAuthorizedRole_*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SourceInstanceARN" : "${ec2:SourceInstanceARN}"
        },
        "ForAnyValue:StringEquals" : {
          "sts:TransitiveTagKeys" : "SourceInstanceARN"
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticDisasterRecoveryReplicationServerPolicy

Descrição: esta política está associada ao perfil de instância do servidor de replicação do Elastic Disaster Recovery. Essa política permite que os servidores de replicação do Elastic Disaster Recovery (DRS), que são instâncias EC2 lançadas pelo Elastic Disaster Recovery, se comuniquem com o serviço DRS e criem snapshots do EBS no seu. Conta da AWS Uma função do IAM com essa política é anexada (como um perfil de instância do EC2) pela Elastic Disaster Recovery aos servidores de replicação do DRS, que são automaticamente iniciados e encerrados pelo DRS, conforme necessário. Os servidores de replicação DRS são usados para facilitar a replicação de dados de seus servidores externos para AWS, como parte do processo de recuperação gerenciado pelo DRS. Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM.

`AWSElasticDisasterRecoveryReplicationServerPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryReplicationServerPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 17 de novembro de 2021, 13:34 UTC

- Hora da edição: 27 de novembro de 2023, 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReplicationServerPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentSnapshotCreditsForDrs",
        "drs:DescribeReplicationServerAssociationsForDrs",
```

```
        "drs:DescribeSnapshotRequestsForDrs",
        "drs:BatchDeleteSnapshotRequestForDrs",
        "drs:NotifyAgentAuthenticationForDrs",
        "drs:BatchCreateVolumeSnapshotGroupForDrs",
        "drs:UpdateAgentReplicationProcessStateForDrs",
        "drs:NotifyAgentReplicationProgressForDrs",
        "drs:NotifyAgentConnectedForDrs",
        "drs:NotifyAgentDisconnectedForDrs",
        "drs:NotifyVolumeEventForDrs",
        "drs:SendVolumeStatsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy5",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSReplicationServerPolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSReplicationServerPolicy7",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticDisasterRecoveryServiceRolePolicy

Descrição: Essa política permite que o Elastic Disaster Recovery gerencie AWS recursos em seu nome.

`AWSElasticDisasterRecoveryServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 17 de novembro de 2021, 10:56 UTC
- Horário editado: 05 de janeiro de 2025, 14:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSServiceRolePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy3",
      "Effect" : "Allow",
```

```
      "Action" : [
        "drs:CreateRecoveryInstanceForDrs",
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy4",
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy5",
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeAttribute",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeDhcpOptions",
```

```
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy10",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "DRSServiceRolePolicy13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy16",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "DRSServiceRolePolicy20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Sid" : "DRSServiceRolePolicy25",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryReplicationServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy28",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy29",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy30",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy31",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "DRSServiceRolePolicy32",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy33",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticDisasterRecoveryStagingAccountPolicy

Descrição: Essa política permite acesso somente para leitura aos recursos do AWS Elastic Disaster Recovery (DRS), como servidores de origem e tarefas. Também permite criar um instantâneo convertido e compartilhar esse instantâneo do EBS com uma conta específica.

`AWSElasticDisasterRecoveryStagingAccountPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryStagingAccountPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 26 de maio de 2022, 9:49 UTC
- Hora da edição: 27 de novembro de 2023, 13:07 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSStagingAccountPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/userId" : "${aws:SourceIdentity}"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

Descrição: Essa política é usada pelo AWS Elastic Disaster Recovery (DRS) para recuperar servidores de origem em uma conta de destino separada e permitir o failback. Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM.

`AWSElasticDisasterRecoveryStagingAccountPolicy_v2` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryStagingAccountPolicy_v2` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 05 de janeiro de 2023, 12:11 UTC
- Horário editado: 09 de setembro de 2026, 13:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicyv21",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSStagingAccountPolicyv22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/userId" : "${aws:SourceIdentity}"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "DRSStagingAccountPolicyv23",
      "Effect" : "Allow",
      "Action" : "drs:IssueAgentCertificateForDrs",
      "Resource" : [
        "arn:aws:drs:*:*:source-server/*"
      ]
    },
    {
      "Sid" : "DRSStagingAccountPolicyv24",
      "Effect" : "Allow",
      "Action" : [
        "drs:CreateSourceServerForDrs",
        "drs:DescribeReplicationConfigurationTemplates"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticLoadBalancingClassicServiceRolePolicy

Descrição: Política de função vinculada ao serviço para o plano de controle do AWS Elastic Load Balancing - Classic

`AWSElasticLoadBalancingClassicServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 19 de setembro de 2017, 22:36 UTC
- Hora da edição: 07 de outubro de 2019, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
```

```
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElasticLoadBalancingServiceRolePolicy

Descrição: Política de função vinculada ao serviço para o plano de controle do AWS Elastic Load Balancing

`AWSElasticLoadBalancingServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 19 de setembro de 2017, 22:19 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses",
        "ec2:ReleaseAddress",
        "ec2:UnassignIpv6Addresses",
```

```
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeAvailabilityZones",
        "ec2:AllocateIpamPoolCidr",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "outposts:GetOutpostInstanceTypes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaConnectCreateBridge

Descrição: Fornece acesso total para criar MediaConnect Gateway Bridges e todos os seus sub-recursos associados.

`AWSElementalMediaConnectCreateBridge` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaConnectCreateBridge` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 19 de março de 2026, 16:57 UTC
- Horário editado: 19 de março de 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectCreateBridge`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:CreateBridge",
        "mediaconnect:AddBridgeSources",
        "mediaconnect:AddBridgeOutputs"
      ],
      "Resource" : [
        "arn:aws:mediaconnect:*:*:bridge:*:*",
        "arn:aws:mediaconnect:*:*:bridge:*:*/bridgeSource/*",
        "arn:aws:mediaconnect:*:*:bridge:*:*/bridgeOutput/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaConnectCreateFlow

Descrição: Fornece acesso total para criar MediaConnect fluxos e todos os sub-recursos associados.

`AWSElementalMediaConnectCreateFlow` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaConnectCreateFlow` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 19 de março de 2026, 16:57 UTC
- Horário editado: 19 de março de 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectCreateFlow`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "mediaconnect.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "mediaconnect:CreateFlow",
        "mediaconnect:AddFlowSources",
        "mediaconnect:AddFlowOutputs",
        "mediaconnect:GrantFlowEntitlements",
        "mediaconnect:AddFlowMediaStreams",
        "mediaconnect:AddFlowVpcInterfaces",
        "mediaconnect:TagResource"
      ],
      "Resource" : [
        "arn:aws:mediaconnect:*:*:flow:*:*",
        "arn:aws:mediaconnect:*:*:source:*:*",
        "arn:aws:mediaconnect:*:*:output:*:*",
        "arn:aws:mediaconnect:*:*:entitlement:*:*",
        "arn:aws:mediaconnect:*:*:flow:*:*/vpcInterface/*",
        "arn:aws:mediaconnect:*:*:flow:*:*/mediaStream/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaConnectDeleteBridge

Descrição: Fornece acesso total para excluir MediaConnect Gateway Bridges e todos os seus sub-recursos associados.

`AWSElementalMediaConnectDeleteBridge` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaConnectDeleteBridge` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 19 de março de 2026, 19:57 UTC
- Horário editado: 19 de março de 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectDeleteBridge`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DeleteBridge",
        "mediaconnect:RemoveBridgeSource",
        "mediaconnect:RemoveBridgeOutput"
      ],
      "Resource" : [
        "arn:aws:mediaconnect:*:*:bridge:*:*",
        "arn:aws:mediaconnect:*:*:bridge:*:*/bridgeSource/*",
        "arn:aws:mediaconnect:*:*:bridge:*:*/bridgeOutput/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaConnectDeleteFlow

Descrição: fornece acesso total para excluir MediaConnect fluxos e todos os sub-recursos associados.

`AWSElementalMediaConnectDeleteFlow` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaConnectDeleteFlow` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 19 de março de 2026, 19:57 UTC
- Horário editado: 19 de março de 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectDeleteFlow`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DeleteFlow",
        "mediaconnect:RemoveFlowSource",
        "mediaconnect:RemoveFlowOutput",
        "mediaconnect:RevokeFlowEntitlement",
        "mediaconnect:RemoveFlowMediaStream",
        "mediaconnect:RemoveFlowVpcInterface"
      ],
      "Resource" : [
        "arn:aws:mediaconnect:*:*:flow:*:*",
        "arn:aws:mediaconnect:*:*:source:*:*",
        "arn:aws:mediaconnect:*:*:output:*:*",
        "arn:aws:mediaconnect:*:*:entitlement:*:*",
        "arn:aws:mediaconnect:*:*:flow:*:*/vpcInterface/*",
        "arn:aws:mediaconnect:*:*:flow:*:*/mediaStream/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaConnectFullAccess

Descrição: Fornece acesso total aos MediaConnect recursos AWS elementares.

`AWSElementalMediaConnectFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaConnectFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 12 de fevereiro de 2025, 20:07 UTC
- Horário editado: 12 de fevereiro de 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaConnectReadOnlyAccess

Descrição: Fornece acesso somente para leitura aos recursos AWS elementares MediaConnect .

`AWSElementalMediaConnectReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaConnectReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 12 de fevereiro de 2025, 20:07 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:ListBridges",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGatewayInstances",
        "mediaconnect:ListGateways",
        "mediaconnect:ListOfferings",
```

```
        "mediaconnect:ListReservations",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeFlowSourceMetadata",
        "mediaconnect:DescribeFlowSourceThumbnail",
        "mediaconnect:DescribeGateway",
        "mediaconnect:DescribeGatewayInstance",
        "mediaconnect:DescribeOffering",
        "mediaconnect:DescribeReservation",
        "mediaconnect:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaConvertFullAccess

Descrição: Fornece acesso total ao AWS Elemental MediaConvert por meio do SDK Console de gerenciamento da AWS e.

`AWSElementalMediaConvertFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaConvertFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de junho de 2018, 19:25 UTC

- Hora da edição: 10 de junho de 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "mediaconvert.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaConvertReadOnly

Descrição: Fornece acesso somente para leitura ao AWS Elemental MediaConvert por meio do SDK Console de gerenciamento da AWS e.

`AWSElementalMediaConvertReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaConvertReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de junho de 2018, 19:25 UTC
- Hora da edição: 10 de junho de 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:DescribeEndpoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaLiveFullAccess

Descrição: Fornece acesso total aos recursos AWS elementares MediaLive

`AWSElementalMediaLiveFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaLiveFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de julho de 2020, 17:07 UTC
- Hora da edição: 08 de julho de 2020, 17:07 UTC

- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "medialive:*",
    "Resource" : "*"
  }
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaLiveReadOnly

Descrição: Fornece acesso somente para leitura aos AWS recursos elementares MediaLive

`AWSElementalMediaLiveReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaLiveReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de julho de 2020, 16:38 UTC
- Hora da edição: 22 de julho de 2024, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSElementalMediaLiveReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "medialive:Get*",
        "medialive:List*",
        "medialive:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaPackageFullAccess

Descrição: Fornece acesso total aos recursos AWS elementares MediaPackage

`AWSElementalMediaPackageFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaPackageFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de dezembro de 2017, 23:39 UTC
- Hora da edição: 29 de dezembro de 2017, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackage:*",
    "Resource" : "*"
  }
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaPackageReadOnly

Descrição: Fornece acesso somente para leitura aos AWS recursos elementares MediaPackage

`AWSElementalMediaPackageReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaPackageReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de dezembro de 2017, 0:04 UTC
- Hora da edição: 30 de dezembro de 2017, 0:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
```

```
    "Effect" : "Allow",
    "Action" : [
      "mediapackage:List*",
      "mediapackage:Describe*"
    ],
    "Resource" : "*"
  }
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaPackageV2FullAccess

Descrição: Fornece acesso total aos recursos do AWS Elemental MediaPackage V2.

`AWSElementalMediaPackageV2FullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaPackageV2FullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de julho de 2023, 20:29 UTC
- Hora da edição: 25 de julho de 2023, 20:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaPackageV2ReadOnly

Descrição: Fornece acesso somente para leitura aos recursos do AWS Elemental MediaPackage V2.

`AWSElementalMediaPackageV2ReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaPackageV2ReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de julho de 2023, 20:31 UTC

- Hora da edição: 25 de julho de 2023, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaStoreFullAccess

Descrição: fornece acesso completo de leitura e gravação a todas as MediaStore APIs

`AWSElementalMediaStoreFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaStoreFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 05 de março de 2018, 23:15 UTC
- Hora da edição: 05 de março de 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaStoreReadOnly

Descrição: fornece permissões somente de leitura para APIs MediaStore

`AWSElementalMediaStoreReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaStoreReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de março de 2018, 19:48 UTC
- Hora da edição: 08 de março de 2018, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaTailorFullAccess

Descrição: Fornece acesso total aos recursos AWS elementares MediaTailor

`AWSElementalMediaTailorFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaTailorFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de novembro de 2021, 0:04 UTC

- Hora da edição: 23 de novembro de 2021, 0:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediatailor:*",
    "Resource" : "*"
  }
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSElementalMediaTailorReadOnly

Descrição: Fornece acesso somente para leitura aos AWS recursos elementares MediaTailor

`AWSElementalMediaTailorReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSElementalMediaTailorReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de novembro de 2021, 0:05 UTC
- Hora da edição: 23 de novembro de 2021, 0:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediatailor:List*",
      "mediatailor:Describe*",
      "mediatailor:Get*"
    ],
    "Resource" : "*"
  }
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSEnhancedClassicNetworkingMangementPolicy

Descrição: política para habilitar o recurso de gerenciamento de rede clássico aprimorado.

`AWSEnhancedClassicNetworkingMangementPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 20 de setembro de 2017, 17:29 UTC
- Hora da edição: 20 de setembro de 2017, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSEntityResolutionConsoleFullAccess

Descrição: Fornece ao console acesso total à Resolução de AWS Entidades e aos serviços relacionados.

`AWSEntityResolutionConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSEntityResolutionConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de agosto de 2023, 17:54 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EntityResolutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "entityresolution:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSourcesConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetSchema",
        "glue:SearchTables",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3BucketsConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3SourcesConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListBucketVersions",
        "s3:GetBucketVersioning"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TaggingConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListRolesToPickRoleForPassing",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToEntityResolutionService",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*entityresolution*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "entityresolution.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "ManageEventBridgeRules",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/entity-resolution-automatic*"
      ]
    },
    {
      "Sid" : "ADXReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetDataSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CustomerProfilesIntegrationReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:ListInstances",
        "profile:ListDomains",
        "profile:GetDomain",
        "profile:ListIntegrations",
        "profile:ListAccountIntegrations",
        "profile:ListProfileObjectTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CustomerProfilesIntegrationWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "profile:PutProfileObjectType"
      ],
      "Resource" : [
```

```
        "arn:aws:profile:*:*:domains/*/object-types/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSEntityResolutionConsoleReadOnlyAccess

Descrição: Fornece acesso somente para leitura à Resolução de AWS Entidades por meio do. Console de gerenciamento da AWS

`AWSEntityResolutionConsoleReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSEntityResolutionConsoleReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de agosto de 2023, 18:18 UTC
- Hora da edição: 17 de agosto de 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EntityResolutionRead",
      "Effect" : "Allow",
      "Action" : [
        "entityresolution:Get*",
        "entityresolution:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSFaultInjectionSimulatorEC2Access

Descrição: esta política concede ao Fault Injection Simulator Service permissão no EC2 e em outros serviços necessários para realizar ações do FIS.

`AWSFaultInjectionSimulatorEC2Access` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSFaultInjectionSimulatorEC2Access` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 26 de outubro de 2022, 20:39 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowEc2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:SendSpotInstanceInterruptions",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "AllowEc2InstancesWithEncryptedEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
```

```
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSSMSendOnEc2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Sid" : "AllowSSMStopOnEc2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:ListCommands"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSFaultInjectionSimulatorECSAccess

Descrição: esta política concede ao Fault Injection Simulator Service permissão no ECS e em outros serviços necessários para realizar ações do FIS.

`AWSFaultInjectionSimulatorECSAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSFaultInjectionSimulatorECSAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 26 de outubro de 2022, 20:37 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Clusters",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:ListContainerInstances"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "Tasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTasks",
        "ecs:StopTask"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*/*"
      ]
    },
    {
      "Sid" : "ContainerInstances",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateContainerInstancesState"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:container-instance/*/*"
      ]
    },
    {
      "Sid" : "ListTasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTasks"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSend",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Sid" : "SSMList",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeContainerInstances",
      "Effect" : "Allow",
      "Action" : "ecs:DescribeContainerInstances",
      "Resource" : "arn:aws:ecs:*:*:container-instance/*/*"
    },
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
```

```
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSFaultInjectionSimulatorEKSAccess

Descrição: esta política concede ao Fault Injection Simulator Service permissão no EKS e em outros serviços necessários para realizar ações do FIS.

`AWSFaultInjectionSimulatorEKSAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSFaultInjectionSimulatorEKSAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 26 de outubro de 2022, 20:34 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "DescribeNodeGroup",
      "Effect" : "Allow",
      "Action" : "eks:DescribeNodegroup",
      "Resource" : "arn:aws:eks:*:*:nodegroup/*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
```

```
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSFaultInjectionSimulatorNetworkAccess

Descrição: esta política concede ao Fault Injection Simulator Service permissão na rede do EC2 e em outros serviços necessários para realizar ações do FIS.

`AWSFaultInjectionSimulatorNetworkAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSFaultInjectionSimulatorNetworkAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 26 de outubro de 2022, 20:32 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateTagsOnNetworkAcl",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkAcl",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkAcl",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkAcl",
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteNetworkAcl",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkAclOnVpc",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkAcl",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "VpcActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReplaceNetworkAclAssociation",
      "Effect" : "Allow",
      "Action" : "ec2:ReplaceNetworkAclAssociation",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-acl/*"
      ]
    },
    {
      "Sid" : "GetManagedPrefixListEntries",
      "Effect" : "Allow",
      "Action" : "ec2:GetManagedPrefixListEntries",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*"
```

```
    },
    {
      "Sid" : "CreateRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:CreateRouteTable",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRouteTableOnVpc",
      "Effect" : "Allow",
      "Action" : "ec2:CreateRouteTable",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "CreateTagsOnRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateRouteTable",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnPrefixList",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateManagedPrefixList",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRoute",
      "Effect" : "Allow",
      "Action" : "ec2:CreateRoute",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "CreateNetworkInterfaceOnSubnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "DeleteNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateManagedPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:CreateManagedPrefixList",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteManagedPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteManagedPrefixList",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ModifyManagedPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:ModifyManagedPrefixList",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "ReplaceRouteTableAssociation",
      "Effect" : "Allow",
      "Action" : "ec2:ReplaceRouteTableAssociation",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "AssociateRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:AssociateRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "DisassociateRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:DisassociateRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DisassociateRouteTableOnSubnet",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:DisassociateRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "ModifyVpcEndpointOnRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:ModifyVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVpcEndpoint",
      "Effect" : "Allow",
      "Action" : "ec2:ModifyVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ]
    },
    {
      "Sid" : "TransitGatewayRouteTableAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:AssociateTransitGatewayRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSFaultInjectionSimulatorRDSAccess

Descrição: esta política concede ao Fault Injection Simulator Service permissão no RDS e em outros serviços necessários para realizar ações do FIS.

`AWSFaultInjectionSimulatorRDSAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSFaultInjectionSimulatorRDSAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 26 de outubro de 2022, 20:30 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFailover",
      "Effect" : "Allow",
      "Action" : [
        "rds:FailoverDBCluster"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "AllowReboot",
      "Effect" : "Allow",
      "Action" : [
        "rds:RebootDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
    },
    {
      "Sid" : "DescribeResources",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSFaultInjectionSimulatorSSMAccess

Descrição: esta política concede ao Fault Injection Simulator Service permissão no SSM e em outros serviços necessários para realizar ações do FIS.

`AWSFaultInjectionSimulatorSSMAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSFaultInjectionSimulatorSSMAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 26 de outubro de 2022, 15:33 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSFinSpaceServiceRolePolicy

Descrição: Política para permitir o acesso AWS service (Serviço da AWS) e os recursos usados ou gerenciados pela Amazon FinSpace

`AWSFinSpaceServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 12 de maio de 2023, 16:42 UTC
- Hora da edição: 1º de dezembro de 2023, 21:05 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSFinSpaceServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/FinSpace",
            "AWS/Usage"
          ]
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSFMAdminFullAccess

Descrição: Acesso total para AWS FM Administrator

`AWSFMAdminFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSFMAdminFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de maio de 2018, 18:06 UTC
- Hora da edição: 20 de outubro de 2022, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fms:*",
        "waf:*",
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
```

```
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:CheckCapacity",
        "wafv2:PutLoggingConfiguration",
        "wafv2:ListAvailableManagedRuleGroupVersions",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:ListRuleGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fms.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListDelegatedAdministrators",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "fms.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSFMAdminReadOnlyAccess

Descrição: Acesso somente de leitura para o AWS FM Administrator, que permite monitorar as operações de AWS FM

`AWSFMAdminReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSFMAdminReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 09 de maio de 2018, 20:07 UTC
- Hora da edição: 31 de outubro de 2022, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fms:Get*",
        "fms:List*",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:CheckCapacity",
        "wafv2:ListAvailableManagedRuleGroupVersions",
```

```
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:ListRuleGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "fms.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSFMMemberReadOnlyAccess

Descrição: Fornece acesso somente para leitura às ações do AWS WAF para contas de membros AWS do Firewall Manager

`AWSFMMemberReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSFMMemberReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de maio de 2018, 21:05 UTC
- Hora da edição: 09 de maio de 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSForWordPressPluginPolicy

Descrição: Política gerenciada AWS para o plugin For Wordpress

`AWSForWordPressPluginPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSForWordPressPluginPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de outubro de 2019, 0:27 UTC
- Horário editado: 03 de setembro de 2026, 20:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Permissions1",
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech",
        "polly:DescribeVoices",
        "translate:TranslateText"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Permissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:CreateBucket",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::audio_for_wordpress*",
        "arn:aws:s3:::audio-for-wordpress*"
      ]
    },
    {
      "Sid" : "Permissions3",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:DescribeCertificate",
        "acm:RequestCertificate",
        "cloudformation:CreateStack",
        "cloudfront:ListDistributions"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "us-east-1"
        }
      }
    },
    {
      "Sid" : "Permissions4",
      "Effect" : "Allow",
      "Action" : [
        "acm:DeleteCertificate",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:UpdateStack",
        "cloudfront:CreateDistribution",
        "cloudfront:CreateInvalidation",
        "cloudfront:DeleteDistribution",
        "cloudfront:GetDistribution",
        "cloudfront:GetInvalidation",
        "cloudfront:TagResource",
        "cloudfront:UpdateDistribution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/createdBy" : "AWSForWordPressPlugin"
        }
      }
    },
    {
      "Sid" : "CloudFormationTagOnCreateStack",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "us-east-1",
          "cloudformation:CreateAction" : "CreateStack"
        }
      }
```

```
    },
    {
      "Sid" : "CloudFormationTagOnUpdateStack",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/createdBy" : "AWSForWordPressPlugin",
          "cloudformation:CreateAction" : "UpdateStack"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSGitSyncServiceRolePolicy

Descrição: Política que permite que o AWS Code Connections sincronize conteúdo do seu repositório git

`AWSGitSyncServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 16 de novembro de 2023, 17:05 UTC
- Hora da edição: 26 de abril de 2024, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSGlobalAcceleratorSLRPolicy

Descrição: Política que concede permissões ao AWS Global Accelerator para gerenciar interfaces de rede elástica e grupos de segurança do EC2.

`AWSGlobalAcceleratorSLRPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 05 de abril de 2019, 19:39 UTC
- Horário editado: 29 de outubro de 2024, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "EC2Action1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSServiceName" : "GlobalAccelerator"
        }
      }
    },
    {
      "Sid" : "EC2Action3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElbAction1",
```

```
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action4",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSGlueConsoleFullAccess

Descrição: Fornece acesso total ao AWS Glue por meio do Console de gerenciamento da AWS

`AWSGlueConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSGlueConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de agosto de 2017, 13:37 UTC
- Horário editado: 10 de setembro de 2026, 20:27 UTC

- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseAppPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBSubnetGroups",
        "s3:ListAllMyBuckets",
```

```
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplateSummary",
        "dynamodb:ListTables",
        "kms:ListAliases",
        "kms:DescribeKey",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListDashboards",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:DescribeRecipe"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*"
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
        },
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSGlueConsoleSageMakerNotebookFullAccess

Descrição: Fornece acesso total ao AWS Glue por meio do Console de gerenciamento da AWS e acesso às instâncias do notebook sagemaker.

`AWSGlueConsoleSageMakerNotebookFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSGlueConsoleSageMakerNotebookFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 05 de outubro de 2018, 17:52 UTC
- Horário editado: 10 de setembro de 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "iam:ListRoles",
        "iam:ListRolePolicies",
```

```
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:CreateNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "rds:DescribeDBInstances",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplateSummary",
        "dynamodb:ListTables",
        "kms:ListAliases",
        "kms:DescribeKey",
        "sagemaker:ListNotebookInstances",
        "cloudformation:ListStacks",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListDashboards"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::*/*aws-glue-*/*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*"
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StopNotebookInstance",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:ListTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance/aws-glue-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:ListNotebookInstanceLifecycleConfigs"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/aws-glue-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
        },
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "aws-glue-*"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
```

```
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceSageMakerNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
```

```
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AwsGlueDataBrewFullAccessPolicy

Descrição: Fornece acesso total ao AWS Glue DataBrew por meio do Console de gerenciamento da AWS. Também fornece acesso selecionado a serviços relacionados (por exemplo, S3, KMS, Glue).

`AwsGlueDataBrewFullAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AwsGlueDataBrewFullAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de novembro de 2020, 16:51 UTC
- Hora da edição: 04 de fevereiro de 2022, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "databrew:CreateDataset",
        "databrew:DescribeDataset",
        "databrew:ListDatasets",
        "databrew:UpdateDataset",
        "databrew:DeleteDataset",
        "databrew:CreateProject",
        "databrew:DescribeProject",
        "databrew:ListProjects",
        "databrew:StartProjectSession",
        "databrew:SendProjectSessionAction",
        "databrew:UpdateProject",
        "databrew:DeleteProject",
        "databrew:CreateRecipe",
        "databrew:DescribeRecipe",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:PublishRecipe",
        "databrew:UpdateRecipe",
        "databrew:BatchDeleteRecipeVersion",
        "databrew:DeleteRecipeVersion",
        "databrew:CreateRecipeJob",
        "databrew:CreateProfileJob",
        "databrew:DescribeJob",
        "databrew:DescribeJobRun",
        "databrew:ListJobRuns",
        "databrew:ListJobs",
        "databrew:StartJobRun",
        "databrew:StopJobRun",
        "databrew:UpdateProfileJob",
        "databrew:UpdateRecipeJob",
        "databrew:DeleteJob",
```

```
        "databrew:CreateSchedule",
        "databrew:DescribeSchedule",
        "databrew:ListSchedules",
        "databrew:UpdateSchedule",
        "databrew:DeleteSchedule",
        "databrew:CreateRuleset",
        "databrew:DeleteRuleset",
        "databrew:DescribeRuleset",
        "databrew:ListRulesets",
        "databrew:UpdateRuleset",
        "databrew:ListTagsForResource",
        "databrew:TagResource",
        "databrew:UntagResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:ListFlows",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetDataCatalogEncryptionSettings",
        "dataexchange:ListDataSets",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:ListRevisionAssets",
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:GetJob",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases",
        "redshift:DescribeClusters",
```

```
        "redshift:DescribeClusterSubnetGroups",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "secretsmanager:ListSecrets",
        "secretsmanager:DescribeSecret",
        "sts:GetCallerIdentity",
        "cloudtrail:LookupEvents",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/AwsGlueDataBrew-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:CreateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*/awsgluedatabrew*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::databrew-public-datasets-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AwsGlueDataBrew-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateRandom"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "databrew.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "databrew!default"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "databrew.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "databrew.amazonaws.com"
          ]
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSGlueDataBrewServiceRole

Descrição: esta política concede permissão ao Glue para executar ações no catálogo de dados do Glue do usuário. Ela também concede permissão para ações do EC2 para permitir que o Glue crie ENI para se conectar a recursos na VPC, além de permitir que o Glue acesse dados registrados no Lake Formation e permissão para acessar o CloudWatch do usuário.

`AWSGlueDataBrewServiceRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSGlueDataBrewServiceRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 04 de dezembro de 2020, 21:26 UTC
- Hora da edição: 20 de março de 2024, 23:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetConnection"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "GluePIIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGetCustomEntityTypes",
        "glue:GetCustomEntityType"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3PublicDatasetAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::databrew-public-datasets-*"
```

```
      ]
    },
    {
      "Sid" : "EC2NetworkingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2DeleteGlueNetworkInterfacePermissions",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws-glue-service-resource" : "*"
        }
      },
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2GlueTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
```

```
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "GlueDatabrewLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws-glue-databrew/*"
      ]
    },
    {
      "Sid" : "LakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSGlueSchemaRegistryFullAccess

Descrição: Fornece acesso total ao AWS Glue Schema Registry Service

`AWSGlueSchemaRegistryFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSGlueSchemaRegistryFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 20 de novembro de 2020, 0:19 UTC
- Hora da edição: 20 de novembro de 2020, 0:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateRegistry",
        "glue:UpdateRegistry",
```

```
        "glue:DeleteRegistry",
        "glue:GetRegistry",
        "glue:ListRegistries",
        "glue:CreateSchema",
        "glue:UpdateSchema",
        "glue:DeleteSchema",
        "glue:GetSchema",
        "glue:ListSchemas",
        "glue:RegisterSchemaVersion",
        "glue:DeleteSchemaVersions",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:ListSchemaVersions",
        "glue:CheckSchemaVersionValidity",
        "glue:PutSchemaVersionMetadata",
        "glue:RemoveSchemaVersionMetadata",
        "glue:QuerySchemaVersionMetadata"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSGlueSchemaRegistryTagsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTags",
        "glue:TagResource",
        "glue:UnTagResource"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:schema/*",
        "arn:aws:glue:*:*:registry/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSGlueSchemaRegistryReadonlyAccess

Descrição: Fornece acesso somente para leitura ao AWS Glue Schema Registry Service

`AWSGlueSchemaRegistryReadonlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSGlueSchemaRegistryReadonlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 20 de novembro de 2020, 0:20 UTC
- Hora da edição: 20 de novembro de 2020, 0:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadonlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryReadonlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetRegistry",
```

```
        "glue:ListRegistries",
        "glue:GetSchema",
        "glue:ListSchemas",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:ListSchemaVersions",
        "glue:GetSchemaVersionsDiff",
        "glue:CheckSchemaVersionValidity",
        "glue:QuerySchemaVersionMetadata",
        "glue:GetTags"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSGlueServiceNotebookRole

Descrição: Política para a função de serviço AWS Glue, que permite ao cliente gerenciar o servidor de notebooks

`AWSGlueServiceNotebookRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSGlueServiceNotebookRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 14 de agosto de 2017, 13:37 UTC

- Hora da edição: 09 de outubro de 2023, 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:DeleteDatabase",
        "glue:DeletePartition",
        "glue:DeleteTable",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:CreateConnection",
        "glue:CreateJob",
        "glue:DeleteConnection",
        "glue:DeleteJob",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDevEndpoint",
```

```
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:UpdateJob",
        "glue:BatchDeleteConnection",
        "glue:UpdateConnection",
        "glue:GetUserDefinedFunction",
        "glue:UpdateUserDefinedFunction",
        "glue:GetUserDefinedFunctions",
        "glue:DeleteUserDefinedFunction",
        "glue:CreateUserDefinedFunction",
        "glue:BatchGetPartition",
        "glue:BatchDeletePartition",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteTable",
        "glue:UpdateDevEndpoint",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*",
        "arn:aws:s3:::aws-glue*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSGlueServiceRole

Descrição: Política para a função de serviço AWS Glue, que permite acesso a serviços relacionados, incluindo EC2, S3 e Cloudwatch Logs

`AWSGlueServiceRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSGlueServiceRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 14 de agosto de 2017, 13:37 UTC
- Hora da edição: 11 de setembro de 2023, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
```

```
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
```

```
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AwsGlueSessionUserRestrictedNotebookPolicy

Descrição: fornece permissões que permitem que os usuários criem e usem somente as sessões de notebook associadas ao usuário. Essa política também inclui permissões para permitir explicitamente que os usuários passem uma função de sessão restrita do Glue.

`AwsGlueSessionUserRestrictedNotebookPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AwsGlueSessionUserRestrictedNotebookPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de abril de 2022, 15:24 UTC
- Hora da edição: 15 de agosto de 2024, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NotebokAllowActions0",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
```

```
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}",
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Sid" : "NotebookAllowActions1",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "NotebookAllowActions2",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
```

```
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Sid" : "NotebookAllowActions3",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "NotebookDenyActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "NotebookPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AwsGlueSessionServiceRoleUserRestrictedForNotebook*",
        "arn:aws:iam::*:role/AwsGlueSessionUserRestrictedNotebookServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AwsGlueSessionUserRestrictedNotebookServiceRole

Descrição: Fornece acesso total a todos os recursos do AWS Glue, exceto às sessões. Permite que os usuários criem e usem somente as sessões de caderno que estejam associadas ao usuário. Essa política também inclui outras permissões necessárias ao AWS Glue para gerenciar os recursos do Glue em outros AWS serviços.

`AwsGlueSessionUserRestrictedNotebookServiceRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AwsGlueSessionUserRestrictedNotebookServiceRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 18 de abril de 2022, 15:27 UTC
- Hora da edição: 15 de agosto de 2024, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
```

```
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}",
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
```

```
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
```

```
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AwsGlueSessionUserRestrictedPolicy

Descrição: fornece permissões que permitem que os usuários criem e usem somente as sessões interativas associadas ao usuário. Essa política também inclui permissões para permitir explicitamente que os usuários passem uma função de sessão restrita do Glue.

`AwsGlueSessionUserRestrictedPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AwsGlueSessionUserRestrictedPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 14 de abril de 2022, 21:31 UTC
- Hora da edição: 5 de agosto de 2024, 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}",
          "aws:RequestTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowCompletionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowListSessions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DenyTagActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AwsGlueSessionServiceRoleUserRestricted*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AwsGlueSessionUserRestrictedServiceRole

Descrição: Fornece acesso total a todos os recursos do AWS Glue, exceto às sessões. Permite que os usuários criem e usem somente as sessões interativas associadas ao usuário. Essa política também inclui outras permissões necessárias ao AWS Glue para gerenciar os recursos do Glue em outros AWS serviços.

`AwsGlueSessionUserRestrictedServiceRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AwsGlueSessionUserRestrictedServiceRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 14 de abril de 2022, 21:30 UTC
- Hora da edição: 5 de agosto de 2024, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Sid" : "AllowCompletionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "AllowSessionActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}",
          "aws:RequestTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowStatementActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
```

```
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowListSessionsAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DenyTagActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Sid" : "AllowS3ObjectCrawlerActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Sid" : "AllowLogsActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Sid" : "AllowTagsActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
```

```
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSGrafanaAccountAdministrator

Descrição: fornece acesso ao Amazon Grafana para criar e gerenciar espaços de trabalho para toda a organização.

`AWSGrafanaAccountAdministrator` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSGrafanaAccountAdministrator` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de fevereiro de 2021, 0:20 UTC

- Hora da edição: 15 de fevereiro de 2022, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaOrganizationAdmin",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaIAMGetRolePermission",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaIAMPassRolePermission",
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "grafana.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSGrafanaConsoleReadOnlyAccess

Descrição: acesso a operações somente leitura no Amazon Grafana.

`AWSGrafanaConsoleReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSGrafanaConsoleReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de fevereiro de 2021, 0:10 UTC
- Hora da edição: 15 de fevereiro de 2022, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaConsoleReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:Describe*",
        "grafana:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSGrafanaWorkspacePermissionManagement

Descrição: Fornece somente a capacidade de atualizar as permissões de usuário e grupo para espaços de trabalho do AWS Grafana.

`AWSGrafanaWorkspacePermissionManagement` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSGrafanaWorkspacePermissionManagement` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de fevereiro de 2021, 0:15 UTC
- Hora da edição: 15 de março de 2023, 22:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:UpdatePermissions",
        "grafana:ListPermissions",
        "grafana:ListWorkspaces"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces*"
    },
    {
      "Sid" : "IAMIdentityCenterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:ListDirectoryAssociations",
        "sso:GetManagedApplicationInstance",
```

```
        "sso:ListProfiles",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso-directory:DescribeUser",
        "sso-directory:DescribeGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSGrafanaWorkspacePermissionManagementV2

Descrição: fornece a capacidade de atualizar as permissões de usuários e grupos do Centro de Identidade (IdC) do IAM para espaços de trabalho do Amazon Managed Grafana.

`AWSGrafanaWorkspacePermissionManagementV2` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSGrafanaWorkspacePermissionManagementV2` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 5 de janeiro de 2024, 18:39 UTC
- Hora da edição: 5 de janeiro de 2024, 18:39 UTC

- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:UpdatePermissions",
        "grafana:ListPermissions",
        "grafana:ListWorkspaces"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces*"
    },
    {
      "Sid" : "IAMIdentityCenterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:ListDirectoryAssociations",
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso-directory:DescribeUser",
        "sso-directory:DescribeGroup"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSGreengrassFullAccess

Descrição: Essa política dá acesso total às ações de configuração, gerenciamento e implantação do AWS Greengrass

`AWSGreengrassFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSGreengrassFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 03 de maio de 2017, 0:47 UTC
- Hora da edição: 03 de maio de 2017, 0:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "greengrass:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSGreengrassReadOnlyAccess

Descrição: Essa política fornece acesso somente para leitura às ações de configuração, gerenciamento e implantação do AWS Greengrass.

`AWSGreengrassReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSGreengrassReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de outubro de 2018, 16:01 UTC
- Hora da edição: 30 de outubro de 2018, 16:01 UTC

- ARN: `arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "greengrass:List*",
        "greengrass:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSGreengrassResourceAccessRolePolicy

Descrição: Política para a função de serviço do AWS Greengrass, que permite acesso a serviços relacionados, incluindo sombras de coisas do AWS Lambda e da AWS IoT.

`AWSGreengrassResourceAccessRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSGreengrassResourceAccessRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 14 de fevereiro de 2017, 21:17 UTC
- Hora da edição: 14 de novembro de 2018, 0:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGreengrassAccessToShadows",
      "Action" : [
        "iot:DeleteThingShadow",
        "iot:GetThingShadow",
        "iot:UpdateThingShadow"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iot:*:*:thing/GG_*",
        "arn:aws:iot:*:*:thing/*-gcm",
        "arn:aws:iot:*:*:thing/*-gda",
        "arn:aws:iot:*:*:thing/*-gci"
      ]
```

```
    },
    {
      "Sid" : "AllowGreengrassToDescribeThings",
      "Action" : [
        "iot:DescribeThing"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iot:*:*:thing/*"
    },
    {
      "Sid" : "AllowGreengrassToDescribeCertificates",
      "Action" : [
        "iot:DescribeCertificate"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iot:*:*:cert/*"
    },
    {
      "Sid" : "AllowGreengrassToCallGreengrassServices",
      "Action" : [
        "greengrass:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassToGetLambdaFunctions",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassToGetGreengrassSecrets",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
    },
    {
      "Sid" : "AllowGreengrassAccessToS3Objects",
```

```
      "Action" : [
        "s3:GetObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::*Greengrass*",
        "arn:aws:s3:::*GreenGrass*",
        "arn:aws:s3:::*greengrass*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowGreengrassAccessToS3BucketLocation",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassAccessToSageMakerTrainingJobs",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSGroundStationAgentInstancePolicy

Descrição: fornece as permissões da instância de endpoint do Dataflow para usar o AWS Ground Station Agent

`AWSGroundStationAgentInstancePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSGroundStationAgentInstancePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de março de 2023, 15:23 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "groundstation:RegisterAgent",
        "groundstation:UpdateAgentStatus",
        "groundstation:GetAgentConfiguration",
        "groundstation:GetAgentTaskResponseUrl"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWS Health_EventProcessorServiceRolePolicy

Descrição: permite que o AWS Health ative o recurso de processador de eventos Health.

`AWSHealth_EventProcessorServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 13 de janeiro de 2023, 19:24 UTC
- Hora da edição: 13 de janeiro de 2023, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "event-processor.health.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSHealthFullAccess

Descrição: permite acesso total às APIs e notificações de AWS saúde e ao painel de saúde pessoal

`AWSHealthFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSHealthFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de dezembro de 2016, 12:30 UTC
- Hora da edição: 16 de novembro de 2020, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "organizations:ServicePrincipal" : "health.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "health:*",
        "organizations:ListAccounts",
        "organizations:ListParents",
        "organizations:DescribeAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "health.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSHealthImagingFullAccess

Descrição: Fornece acesso total ao serviço AWS de imagens de saúde.

`AWSHealthImagingFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSHealthImagingFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de julho de 2023, 23:39 UTC
- Hora da edição: 25 de julho de 2023, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "medical-imaging:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "medical-imaging.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSHealthImagingReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao serviço AWS Health Imaging.

`AWSHealthImagingReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSHealthImagingReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de julho de 2023, 23:40 UTC
- Hora da edição: 01 de agosto de 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "medical-imaging:GetDICOMImportJob",
        "medical-imaging:GetDatastore",
        "medical-imaging:GetImageFrame",
        "medical-imaging:GetImageSet",
        "medical-imaging:GetImageSetMetadata",
        "medical-imaging:ListDICOMImportJobs",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListImageSetVersions",
        "medical-imaging:ListTagsForResource",
        "medical-imaging:SearchImageSets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSHealthImagingServiceRolePolicy

Descrição: Fornece permissões AWS HealthImaging para gerenciar operações de serviço e publicar métricas de serviço

`AWSHealthImagingServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 30 de janeiro de 2026, 18:34 UTC
- Horário editado: 30 de janeiro de 2026, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealthImagingServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/HealthImaging"
        }
      }
```

```
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSHealthOmicsServiceLinkedRolePolicy

Descrição: Política gerenciada para a função vinculada ao Amazon HealthOmics Service

`AWSHealthOmicsServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Tempo de criação: 04 de março de 2026, 22:57 UTC
- Horário editado: 04 de março de 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealthOmicsServiceLinkedRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowEC2DescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowVpcGetActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "AllowCreateNetworkInterfaceWithTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Service" : "HealthOmics"
        }
      }
    },
    {
      "Sid" : "AllowCreateNetworkInterfaceSubnetSecurityGroup",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "AllowCreateTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "AllowDeleteNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Service" : "HealthOmics"
        }
      }
    },
    {
      "Sid" : "AllowAssignUnassignPrivateIpAddresses",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Service" : "HealthOmics"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIAMIdentityCenterAllowListForIdentityContext

Descrição: fornece a lista de ações permitidas para funções assumidas com o contexto de identidade do IAM Identity Center. AWS O Security Token Service (AWS STS) anexa automaticamente essa política às funções assumidas. O contexto de identidades é passado como ProvidedContext.

`AWSIAMIdentityCenterAllowListForIdentityContext` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIAMIdentityCenterAllowListForIdentityContext` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de novembro de 2023, 15:21 UTC
- Hora da edição: 1º de outubro de 2024, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "TrustedIdentityPropagation",
      "Effect" : "Deny",
      "NotAction" : [
        "aoss:APIAccessAll",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreatePreparedStatement",
        "athena:DeleteNamedQuery",
        "athena:DeletePreparedStatement",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:UpdateNamedQuery",
        "athena:UpdatePreparedStatement",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups",
        "elasticmapreduce:GetClusterSessionCredentials",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:ListSteps",
        "es:ESHttpHead",
        "es:ESHttpPost",
        "es:ESHttpGet",
        "es:ESHttpPatch",
```

```
        "es:ESHttpDelete",
        "es:ESHttpPut",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersions",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:SearchTables",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchUpdatePartition",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "lakeformation:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix",
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:StartTroubleshootingAnalysis",
        "q:GetTroubleshootingResults",
        "q:StartTroubleshootingResolutionExplanation",
        "q:UpdateTroubleshootingCommandResult",
        "qapps:CreateQApp",
        "qapps:PredictProblemStatementFromConversation",
```

```
        "qapps:PredictQAppFromProblemStatement",
        "qapps:CopyQApp",
        "qapps:GetQApp",
        "qapps:ListQApps",
        "qapps:UpdateQApp",
        "qapps:DeleteQApp",
        "qapps:AssociateQAppWithUser",
        "qapps:DisassociateQAppFromUser",
        "qapps:ImportDocumentToQApp",
        "qapps:ImportDocumentToQAppSession",
        "qapps:CreateLibraryItem",
        "qapps:GetLibraryItem",
        "qapps:UpdateLibraryItem",
        "qapps:CreateLibraryItemReview",
        "qapps:ListLibraryItems",
        "qapps:CreateSubscriptionToken",
        "qapps:StartQAppSession",
        "qapps:StopQAppSession",
        "qapps:PredictQApp",
        "qapps:ImportDocument",
        "qapps:AssociateLibraryItemReview",
        "qapps:DisassociateLibraryItemReview",
        "qapps:GetQAppSession",
        "qapps:UpdateQAppSession",
        "qapps:GetQAppSessionMetadata",
        "qapps:UpdateQAppSessionMetadata",
        "qapps:TagResource",
        "qapps:ListQAppSessionData",
        "qapps:ExportQAppSessionData",
        "qbusiness:Chat",
        "qbusiness:ChatSync",
        "qbusiness:ListConversations",
        "qbusiness:ListMessages",
        "qbusiness:DeleteConversation",
        "qbusiness:PutFeedback",
        "sts:SetContext"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIAMRoleManagerServiceRolePolicy

Descrição: permite que o IAM Role Manager gerencie recursos em sua conta em seu nome.

`AWSIAMRoleManagerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Tempo de criação: 15 de julho de 2026, 23:57 UTC
- Horário editado: 05 de agosto de 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIAMRoleManagerServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageServiceLinkedAnalyzer",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CreateServiceLinkedAnalyzer",
        "access-analyzer:DeleteServiceLinkedAnalyzer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateAccessAnalyzerServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "access-analyzer.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIdentityCenterExternalManagementPolicy

Descrição: fornece acesso para gerenciar usuários do IAM Identity Center a partir de um provedor externo.

`AWSIdentityCenterExternalManagementPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIdentityCenterExternalManagementPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 22 de novembro de 2025, 00:34 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIdentityCenterExternalManagementPolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IdentityStoreUserCreation",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:CreateUser"
      ],
      "Resource" : [
        "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/IdentityStoreId}",
        "arn:aws:identitystore:::user/*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "identitystore:UserExternalIdIssuers" : [
```

```
            "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/
IdentityStoreId}/provisioningtenant/${aws:PrincipalTag/IdentityStoreExternalIdIssuer}"
          ]
        },
        "Null" : {
          "identitystore:UserExternalIdIssuers" : "false",
          "identitystore:ReservedUserId" : "false"
        }
      }
    },
    {
      "Sid" : "IdentityStoreUserManagement",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:UpdateUser",
        "identitystore:DeleteUser",
        "identitystore:DescribeUser"
      ],
      "Resource" : [
        "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/IdentityStoreId}",
        "arn:aws:identitystore:::user/*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "identitystore:UserExternalIdIssuers" : [
            "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/
IdentityStoreId}/provisioningtenant/${aws:PrincipalTag/IdentityStoreExternalIdIssuer}"
          ]
        },
        "Null" : {
          "identitystore:UserExternalIdIssuers" : "false"
        }
      }
    },
    {
      "Sid" : "IdentityStoreCMKAccess",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : [
            "arn:aws:identitystore::${aws:PrincipalAccount}:identitystore/
${aws:PrincipalTag/IdentityStoreId}"
```

```
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIdentitySyncFullAccess

Descrição: concede acesso total ao serviço Identity Sync

`AWSIdentitySyncFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIdentitySyncFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de março de 2022, 23:29 UTC
- Hora da edição: 23 de março de 2022, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication"
      ],
      "Resource" : "arn:*:ds:*:*:*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile",
        "identity-sync:CreateSyncProfile",
        "identity-sync:GetSyncProfile",
        "identity-sync:StartSync",
        "identity-sync:StopSync",
        "identity-sync:CreateSyncFilter",
        "identity-sync:DeleteSyncFilter",
        "identity-sync:ListSyncFilters",
        "identity-sync:CreateSyncTarget",
        "identity-sync:DeleteSyncTarget",
        "identity-sync:GetSyncTarget",
        "identity-sync:UpdateSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIdentitySyncReadOnlyAccess

Descrição: concede acesso somente leitura ao serviço Identity Sync

`AWSIdentitySyncReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIdentitySyncReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de março de 2022, 23:29 UTC
- Hora da edição: 23 de março de 2022, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
```

```
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSImageBuilderFullAccess

Descrição: fornece acesso total a todas as ações do AWS Image Builder e acesso com escopo de recursos aos AWS serviços relacionados.

`AWSImageBuilderFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSImageBuilderFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário da criação: 20 de dezembro de 2019, 18:25 UTC
- Hora da edição: 13 de abril de 2021, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListLicenseSpecificationsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*imagebuilder*",
        "arn:aws:iam::*:role/*imagebuilder*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
```

```
      "Resource" : "arn:aws:s3::*:*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "imagebuilder.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeVolumes",
        "ec2:DescribeSubnets",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSImageBuilderReadOnlyAccess

Descrição: Fornece acesso somente para leitura a todas as ações do AWS Image Builder.

`AWSImageBuilderReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSImageBuilderReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 19 de dezembro de 2019, 22:29 UTC
- Hora da edição: 19 de dezembro de 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:Get*",
        "imagebuilder:List*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSImportExportFullAccess

Descrição: fornece acesso de leitura e gravação aos trabalhos criados sob a Conta da AWS.

`AWSImportExportFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSImportExportFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "importexport:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSImportExportReadOnlyAccess

Descrição: fornece acesso somente leitura aos trabalhos criados sob a Conta da AWS.

`AWSImportExportReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSImportExportReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "importexport:ListJobs",
        "importexport:GetStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIncidentManagerIncidentAccessServiceRolePolicy

Descrição: Concede ao Gerenciador de Incidentes permissões para ligar para outros AWS serviços como parte do gerenciamento de um incidente.

`AWSIncidentManagerIncidentAccessServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIncidentManagerIncidentAccessServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 13 de novembro de 2023, 0:01 UTC
- Hora da edição: 20 de fevereiro de 2024, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIncidentManagerResolverAccess

Descrição: esta política concede permissões para iniciar, visualizar e atualizar incidentes com acesso total a eventos personalizados e itens relacionados da linha de tempo. Atribua essa política aos usuários que criarão e resolverão incidentes.

`AWSIncidentManagerResolverAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIncidentManagerResolverAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 10 de maio de 2021, 6:12 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC

- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:StartIncident",
        "ssm-contacts:StartEngagement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResponsePlanReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:GetResponsePlan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentRecordResolverPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:UpdateIncidentRecord",
        "ssm-incidents:ListTimelineEvents",
        "ssm-incidents:CreateTimelineEvent",
```

```
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:UpdateTimelineEvent",
        "ssm-incidents:DeleteTimelineEvent",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:UpdateRelatedItems"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIncidentManagerServiceRolePolicy

Descrição: esta política concede permissão ao Incident Manager para gerenciar registros de incidentes e recursos relacionados em seu nome.

`AWSIncidentManagerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 10 de maio de 2021, 3:34 UTC
- Horário editado: 28 de janeiro de 2025, 02:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UpdateIncidentRecordPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:CreateTimelineEvent"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedOpsItemPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AssociateOpsItemRelatedItem"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentEngagementPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-contacts:StartEngagement",
      "Resource" : "*"
    },
    {
      "Sid" : "PutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IncidentManager",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoT1ClickFullAccess

Descrição: Fornece acesso total ao AWS IoT 1-Click.

`AWSIoT1ClickFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoT1ClickFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de maio de 2018, 22:10 UTC
- Hora da edição: 11 de maio de 2018, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoT1ClickReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao AWS IoT 1-Click.

`AWSIoT1ClickReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoT1ClickReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 11 de maio de 2018, 21:49 UTC
- Hora da edição: 11 de maio de 2018, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTAnalyticsFullAccess

Descrição: fornece acesso total ao IoT Analytics.

`AWSIoTAnalyticsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTAnalyticsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de junho de 2018, 23:02 UTC
- Hora da edição: 18 de junho de 2018, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotanalytics:*"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTAnalyticsReadOnlyAccess

Descrição: fornece acesso somente leitura ao IoT Analytics.

`AWSIoTAnalyticsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTAnalyticsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 18 de junho de 2018, 21:37 UTC
- Hora da edição: 18 de junho de 2018, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotanalytics:Describe*",
        "iotanalytics:List*",
        "iotanalytics:Get*",
        "iotanalytics:SampleChannelData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTConfigAccess

Descrição: Essa política dá acesso total às ações de configuração de AWS IoT

`AWSIoTConfigAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTConfigAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de outubro de 2015, 21:52 UTC
- Hora da edição: 27 de setembro de 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigAccess`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:AcceptCertificateTransfer",
        "iot:AddThingToThingGroup",
        "iot:AssociateTargetsWithJob",
        "iot:AttachPolicy",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CancelCertificateTransfer",
        "iot:CancelJob",
        "iot:CancelJobExecution",
        "iot:ClearDefaultAuthorizer",
        "iot:CreateAuthorizer",
        "iot:CreateCertificateFromCsr",
        "iot:CreateJob",
        "iot:CreateKeysAndCertificate",
        "iot:CreateOTAUpdate",
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion",
        "iot:CreateRoleAlias",
        "iot:CreateStream",
        "iot:CreateThing",
        "iot:CreateThingGroup",
        "iot:CreateThingType",
        "iot:CreateTopicRule",
        "iot:DeleteAuthorizer",
        "iot:DeleteCACertificate",
        "iot:DeleteCertificate",
        "iot:DeleteJob",
```

```
        "iot:DeleteJobExecution",
        "iot:DeleteOTAUpdate",
        "iot:DeletePolicy",
        "iot:DeletePolicyVersion",
        "iot:DeleteRegistrationCode",
        "iot:DeleteRoleAlias",
        "iot:DeleteStream",
        "iot:DeleteThing",
        "iot:DeleteThingGroup",
        "iot:DeleteThingType",
        "iot:DeleteTopicRule",
        "iot:DeleteV2LoggingLevel",
        "iot:DeprecateThingType",
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeDefaultAuthorizer",
        "iot:DescribeEndpoint",
        "iot:DescribeEventConfigurations",
        "iot:DescribeIndex",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DescribeRoleAlias",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingRegistrationTask",
        "iot:DescribeThingType",
        "iot:DetachPolicy",
        "iot:DetachPrincipalPolicy",
        "iot:DetachThingPrincipal",
        "iot:DisableTopicRule",
        "iot:EnableTopicRule",
        "iot:GetEffectivePolicies",
        "iot:GetIndexingConfiguration",
        "iot:GetJobDocument",
        "iot:GetLoggingOptions",
        "iot:GetOTAUpdate",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:GetRegistrationCode",
        "iot:GetTopicRule",
        "iot:GetV2LoggingOptions",
        "iot:ListAttachedPolicies",
```

```
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCertificatesByCA",
        "iot:ListIndices",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:ListJobs",
        "iot:ListOTAUpdates",
        "iot:ListOutgoingCertificates",
        "iot:ListPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPolicyVersions",
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListRoleAliases",
        "iot:ListStreams",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroups",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:ListThingRegistrationTaskReports",
        "iot:ListThingRegistrationTasks",
        "iot:ListThings",
        "iot:ListThingsInThingGroup",
        "iot:ListThingTypes",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:RegisterCACertificate",
        "iot:RegisterCertificate",
        "iot:RegisterThing",
        "iot:RejectCertificateTransfer",
        "iot:RemoveThingFromThingGroup",
        "iot:ReplaceTopicRule",
        "iot:SearchIndex",
        "iot:SetDefaultAuthorizer",
        "iot:SetDefaultPolicyVersion",
        "iot:SetLoggingOptions",
        "iot:SetV2LoggingLevel",
        "iot:SetV2LoggingOptions",
        "iot:StartThingRegistrationTask",
        "iot:StopThingRegistrationTask",
        "iot:TestAuthorization",
        "iot:TestInvokeAuthorizer",
```

```
        "iot:TransferCertificate",
        "iot:UpdateAuthorizer",
        "iot:UpdateCACertificate",
        "iot:UpdateCertificate",
        "iot:UpdateEventConfigurations",
        "iot:UpdateIndexingConfiguration",
        "iot:UpdateRoleAlias",
        "iot:UpdateStream",
        "iot:UpdateThing",
        "iot:UpdateThingGroup",
        "iot:UpdateThingGroupsForThing",
        "iot:UpdateAccountAuditConfiguration",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DeleteAccountAuditConfiguration",
        "iot:StartOnDemandAuditTask",
        "iot:CancelAuditTask",
        "iot:DescribeAuditTask",
        "iot:ListAuditTasks",
        "iot:CreateScheduledAudit",
        "iot:UpdateScheduledAudit",
        "iot:DeleteScheduledAudit",
        "iot:DescribeScheduledAudit",
        "iot:ListScheduledAudits",
        "iot:ListAuditFindings",
        "iot:CreateSecurityProfile",
        "iot:DescribeSecurityProfile",
        "iot:UpdateSecurityProfile",
        "iot:DeleteSecurityProfile",
        "iot:AttachSecurityProfile",
        "iot:DetachSecurityProfile",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListActiveViolations",
        "iot:ListViolationEvents",
        "iot:ValidateSecurityProfileBehaviors"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTConfigReadOnlyAccess

Descrição: Essa política fornece acesso somente para leitura às ações de configuração de AWS IoT.

`AWSIoTConfigReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTConfigReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de outubro de 2015, 21:52 UTC
- Hora da edição: 27 de setembro de 2019, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeDefaultAuthorizer",
        "iot:DescribeEndpoint",
        "iot:DescribeEventConfigurations",
        "iot:DescribeIndex",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DescribeRoleAlias",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingRegistrationTask",
        "iot:DescribeThingType",
        "iot:GetEffectivePolicies",
        "iot:GetIndexingConfiguration",
        "iot:GetJobDocument",
        "iot:GetLoggingOptions",
        "iot:GetOTAUpdate",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:GetRegistrationCode",
        "iot:GetTopicRule",
        "iot:GetV2LoggingOptions",
        "iot:ListAttachedPolicies",
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCertificatesByCA",
        "iot:ListIndices",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:ListJobs",
        "iot:ListOTAUpdates",
        "iot:ListOutgoingCertificates",
        "iot:ListPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPolicyVersions",
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListRoleAliases",
```

```
        "iot:ListStreams",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroups",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:ListThingRegistrationTaskReports",
        "iot:ListThingRegistrationTasks",
        "iot:ListThings",
        "iot:ListThingsInThingGroup",
        "iot:ListThingTypes",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:SearchIndex",
        "iot:TestAuthorization",
        "iot:TestInvokeAuthorizer",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuditTask",
        "iot:ListAuditTasks",
        "iot:DescribeScheduledAudit",
        "iot:ListScheduledAudits",
        "iot:ListAuditFindings",
        "iot:DescribeSecurityProfile",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListActiveViolations",
        "iot:ListViolationEvents",
        "iot:ValidateSecurityProfileBehaviors"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTDataAccess

Descrição: Essa política dá acesso total às ações de mensagens da AWS IoT

`AWSIoTDataAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTDataAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de outubro de 2015, 21:51 UTC
- Hora da edição: 23 de junho de 2021, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDataAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:Connect",
        "iot:Publish",
        "iot:Subscribe",
        "iot:Receive",
        "iot:GetThingShadow",
```

```
        "iot:UpdateThingShadow",
        "iot:DeleteThingShadow",
        "iot:ListNamedShadowsForThing"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

Descrição: fornece acesso de gravação a grupos de coisas de IoT e acesso de leitura a certificados de IoT para execução da ação de mitigação ADD_THINGS_TO_THING_GROUP

`AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 07 de agosto de 2019, 17:55 UTC
- Hora da edição: 07 de agosto de 2019, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:ListPrincipalThings",
        "iot:AddThingToThingGroup"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTDeviceDefenderAudit

Descrição: fornece acesso de leitura para IoT e recursos relacionados

`AWSIoTDeviceDefenderAudit` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTDeviceDefenderAudit` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 18 de julho de 2018, 21:17 UTC
- Hora da edição: 25 de novembro de 2019, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:GetLoggingOptions",
        "iot:GetV2LoggingOptions",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:ListPolicies",
        "iot:GetPolicy",
        "iot:GetEffectivePolicies",
        "iot:ListRoleAliases",
        "iot:DescribeRoleAlias",
        "cognito-identity:GetIdentityPoolRoles",
```

```
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetails"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

Descrição: fornece acesso para habilitar o log de IoT para execução da ação de mitigação ENABLE_IOT_LOGGING

`AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço

- Hora da criação: 07 de agosto de 2019, 17:04 UTC
- Hora da edição: 07 de agosto de 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com"
          ]
        }
```

```
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

Descrição: fornece acesso de publicação de mensagens ao tópico do SNS para execução da ação de mitigação PUBLISH_FINDING_TO_SNS

`AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 07 de agosto de 2019, 17:04 UTC
- Hora da edição: 07 de agosto de 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

Descrição: fornece acesso de gravação às políticas de IoT para execução da ação de mitigação REPLACE_DEFAULT_POLICY_VERSION

`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 07 de agosto de 2019, 17:04 UTC
- Hora da edição: 07 de agosto de 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicyVersion"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTDeviceDefenderUpdateCACertMitigationAction

Descrição: fornece acesso de gravação aos certificados de CA de IoT para execução da ação de mitigação UPDATE_CA_CERTIFICATE

`AWSIoTDeviceDefenderUpdateCACertMitigationAction` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTDeviceDefenderUpdateCACertMitigationAction` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 07 de agosto de 2019, 17:05 UTC
- Hora da edição: 07 de agosto de 2019, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:UpdateCACertificate"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

Descrição: fornece acesso de gravação aos certificados de CA de IoT para execução da ação de mitigação UPDATE_DEVICE_CERTIFICATE

`AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 07 de agosto de 2019, 17:06 UTC
- Hora da edição: 07 de agosto de 2019, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:UpdateCertificate"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTDeviceTesterForFreeRTOSFullAccess

Descrição: permite que o AWS IoT Device Tester execute o pacote de qualificação FreeRTOS ao permitir o acesso a serviços, incluindo IoT, S3 e IAM

`AWSIoTDeviceTesterForFreeRTOSFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTDeviceTesterForFreeRTOSFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 12 de fevereiro de 2020, 20:33 UTC
- Hora da edição: 10 de agosto de 2023, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/idt-*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "iot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteThing",
        "iot:AttachThingPrincipal",
        "iot:DeleteCertificate",
        "iot:GetRegistrationCode",
        "iot:CreatePolicy",
        "iot:UpdateCACertificate",
        "s3:ListBucket",
        "iot:DescribeEndpoint",
        "iot:CreateOTAUpdate",
        "iot:CreateStream",
        "signer:ListSigningJobs",
        "acm:ListCertificates",
        "iot:CreateKeysAndCertificate",
        "iot:UpdateCertificate",
        "iot:CreateCertificateFromCsr",
        "iot:DetachThingPrincipal",
        "iot:RegisterCACertificate",
        "iot:CreateThing",
        "iam:ListRoles",
        "iot:RegisterCertificate",
        "iot:DeleteCACertificate",
        "signer:PutSigningProfile",
        "s3:ListAllMyBuckets",
        "signer:ListSigningPlatforms",
        "iot-device-tester:SendMetrics",
        "iot-device-tester:SupportedVersion",
        "iot-device-tester:LatestIdt",
        "iot-device-tester:CheckVersion",
        "iot-device-tester:DownloadTestSuite"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor2",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "signer:StartSigningJob",
        "acm:GetCertificate",
        "signer:DescribeSigningJob",
        "s3:CreateBucket",
        "execute-api:Invoke",
        "s3:DeleteBucket",
        "s3:PutBucketVersioning",
        "signer:CancelSigningProfile"
      ],
      "Resource" : [
        "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
        "arn:aws:signer:*:*:/signing-profiles/*",
        "arn:aws:signer:*:*:/signing-jobs/*",
        "arn:aws:iam::*:role/idt-*",
        "arn:aws:acm:*:*:certificate/*",
        "arn:aws:s3:::idt-*",
        "arn:aws:s3:::afr-ota*"
      ]
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteStream",
        "iot:DeleteCertificate",
        "iot:AttachPolicy",
        "iot:DetachPolicy",
        "iot:DeletePolicy",
        "s3:ListBucketVersions",
        "iot:UpdateCertificate",
        "iot:GetOTAUpdate",
        "iot:DeleteOTAUpdate",
        "iot:DescribeJobExecution"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*",
        "arn:aws:iot:*:*:thinggroup/idt*",
        "arn:aws:iam::*:role/idt-*"
      ]
    },
    {
```

```
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteCertificate",
        "iot:AttachPolicy",
        "iot:DetachPolicy",
        "s3:DeleteObjectVersion",
        "iot:DeleteOTAUpdate",
        "s3:PutObject",
        "s3:GetObject",
        "iot:DeleteStream",
        "iot:DeletePolicy",
        "s3:DeleteObject",
        "iot:UpdateCertificate",
        "iot:GetOTAUpdate",
        "s3:GetObjectVersion",
        "iot:DescribeJobExecution"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*/*",
        "arn:aws:s3:::idt-*/*",
        "arn:aws:iot:*:*:policy/idt*",
        "arn:aws:iam::*:role/idt-*",
        "arn:aws:iot:*:*:otaupdate/idt*",
        "arn:aws:iot:*:*:thing/idt*",
        "arn:aws:iot:*:*:cert/*",
        "arn:aws:iot:*:*:job/*",
        "arn:aws:iot:*:*:stream/*"
      ]
    },
    {
      "Sid" : "VisualEditor5",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*/*",
        "arn:aws:s3:::idt-*/*"
      ]
    },
    {
      "Sid" : "VisualEditor6",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iot:CancelJobExecution"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/*",
        "arn:aws:iot:*:*:thing/idt*"
      ]
    },
    {
      "Sid" : "VisualEditor7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor9",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "VisualEditor11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
```

```
      "Sid" : "VisualEditor12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ssm:DescribeParameters",
        "ssm:GetParameters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "Owner"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateSecurityGroup"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTDeviceTesterForGreengrassFullAccess

Descrição: Permite que o AWS IoT Device Tester execute o pacote de qualificação do AWS Greengrass ao permitir o acesso a serviços relacionados, incluindo Lambda, IoT, API Gateway e IAM

`AWSIoTDeviceTesterForGreengrassFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTDeviceTesterForGreengrassFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 20 de fevereiro de 2020, 21:21 UTC
- Hora da edição: 25 de junho de 2020, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/idt-*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com",
            "lambda.amazonaws.com",
            "greengrass.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "iot:DeleteCertificate",
        "lambda:DeleteFunction",
        "execute-api:Invoke",
        "iot:UpdateCertificate"
      ],
      "Resource" : [
        "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
        "arn:aws:lambda:*:*:function:idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPolicy",
        "iot:DetachPolicy",
```

```
        "iot:DeletePolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor5",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateJob",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DeleteJob"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:job/*"
      ]
    },
    {
      "Sid" : "VisualEditor6",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint",
        "greengrass:*",
        "iam:ListAttachedRolePolicies",
        "iot:CreatePolicy",
        "iot:GetThingShadow",
        "iot:CreateKeysAndCertificate",
        "iot:ListThings",
        "iot:UpdateThingShadow",
        "iot:CreateCertificateFromCsr",
        "iot-device-tester:SendMetrics",
        "iot-device-tester:SupportedVersion",
        "iot-device-tester:LatestIdt",
        "iot-device-tester:CheckVersion",
        "iot-device-tester:DownloadTestSuite"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor7",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iot:DetachThingPrincipal",
        "iot:AttachThingPrincipal"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObjectVersion",
        "s3:ListBucketVersions",
        "s3:CreateBucket",
        "s3:DeleteObject",
        "s3:DeleteBucket"
      ],
      "Resource" : "arn:aws:s3:::idt*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTEventsFullAccess

Descrição: fornece acesso total ao IoT Events.

`AWSIoTEventsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTEventsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 10 de janeiro de 2019, 22:51 UTC
- Hora da edição: 10 de janeiro de 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotevents:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTEventsReadOnlyAccess

Descrição: fornece acesso somente leitura ao IoT Events.

`AWSIoTEventsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTEventsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 10 de janeiro de 2019, 22:50 UTC
- Hora da edição: 23 de setembro de 2019, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotevents:Describe*",
        "iotevents:List*"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTFleetHubFederationAccess

Descrição: acesso à federação para aplicativos do IoT Fleet Hub

`AWSIoTFleetHubFederationAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTFleetHubFederationAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 15 de dezembro de 2020, 8:08 UTC
- Hora da edição: 04 de abril de 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTFleetHubFederationAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeIndex",
        "iot:DescribeThingGroup",
        "iot:GetBucketsAggregation",
        "iot:GetCardinality",
        "iot:GetIndexingConfiguration",
        "iot:GetPercentiles",
        "iot:GetStatistics",
        "iot:SearchIndex",
        "iot:CreateFleetMetric",
        "iot:ListFleetMetrics",
        "iot:DeleteFleetMetric",
        "iot:DescribeFleetMetric",
        "iot:UpdateFleetMetric",
        "iot:DescribeCustomMetric",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListMetricValues",
        "iot:ListThingGroups",
        "iot:ListThingsInThingGroup",
        "iot:ListJobTemplates",
        "iot:DescribeJobTemplate",
        "iot:ListJobs",
        "iot:CreateJob",
        "iot:CancelJob",
        "iot:DescribeJob",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:DescribeJobExecution",
        "iot:ListSecurityProfiles",
        "iot:DescribeSecurityProfile",
        "iot:ListActiveViolations",
        "iot:GetThingShadow",
        "iot:ListNamedShadowsForThing",
        "iot:CancelJobExecution",
        "iot:DescribeEndpoint",
```

```
        "iotfleethub:DescribeApplication",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptionsByTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:iotfleethub*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:iotfleethub*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTFleetwiseServiceRolePolicy

Descrição: Concede permissões a AWS recursos e metadados usados ou gerenciados AWSIoTFleetwise por recursos auxiliares

`AWSIoTFleetwiseServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 21 de setembro de 2022, 23:27 UTC
- Horário editado: 16 de outubro de 2025, 04:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTFleetwiseServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IoTFleetWise",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTFullAccess

Descrição: Essa política dá acesso total à configuração de AWS IoT e às ações de mensagens.

`AWSIoTFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de outubro de 2015, 15:19 UTC
- Hora da edição: 19 de maio de 2022, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:*",
        "iotjobsdata:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTLogging

Descrição: permite a criação de grupos do Amazon CloudWatch Log e de logs de streaming para os grupos

`AWSIoTLogging` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTLogging` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 08 de outubro de 2015, 15:17 UTC
- Hora da edição: 08 de outubro de 2015, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTLogging`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
        "logs:GetLogEvents",
        "logs:DeleteLogStream"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTManagedIntegrationsFullAccess

Descrição: Fornece acesso total às integrações gerenciadas para gerenciamento de dispositivos de AWS IoT e serviços relacionados.

`AWSIoTManagedIntegrationsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTManagedIntegrationsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 05 de março de 2025, 19:22 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTManagedIntegrationsFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iotmanagedintegrations:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
iotmanagedintegrations.amazonaws.com/AWSServiceRoleForIoTManagedIntegrations",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "iotmanagedintegrations.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTManagedIntegrationsRolePolicy

Descrição: fornece integrações gerenciadas para permitir que o AWS IoT Device Management publique registros e métricas em seu nome.

`AWSIoTManagedIntegrationsRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 05 de março de 2025, 21:22 UTC
- Horário editado: 05 de março de 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTManagedIntegrationsRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/iotmanagedintegrations/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchStreams",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/iotmanagedintegrations/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IoTManagedIntegrations",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTOTAUpdate

Descrição: permite acesso para criar um trabalho de AWS IoT e descrever o trabalho do signatário AWS de código

`AWSIoTOTAUpdate` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTOTAUpdate` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 20 de dezembro de 2017, 20:36 UTC
- Hora da edição: 20 de dezembro de 2017, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "iot:CreateJob",
      "signer:DescribeSigningJob"
    ],
    "Resource" : "*"
  }
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIotRoboRunnerFullAccess

Descrição: Essa política concede permissões que permitem acesso total à AWS IoT RoboRunner.

`AWSIotRoboRunnerFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIotRoboRunnerFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2021, 3:54 UTC
- Hora da edição: 23 de fevereiro de 2023, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : "iotroborunner:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/iotroborunner.amazonaws.com/
AWSServiceRoleForIoTRoboRunner",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "iotroborunner.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIotRoboRunnerReadOnly

Descrição: Essa política concede permissões que permitem acesso somente para AWS leitura à IoT. RoboRunner

`AWSIotRoboRunnerReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIotRoboRunnerReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2021, 3:43 UTC

- Hora da edição: 16 de novembro de 2022, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerReadOnly`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotroborunner:GetSite",
        "iotroborunner:GetWorker",
        "iotroborunner:ListWorkerFleets",
        "iotroborunner:ListSites",
        "iotroborunner:ListWorkers",
        "iotroborunner:GetDestination",
        "iotroborunner:GetWorkerFleet",
        "iotroborunner:ListDestinations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIotRoboRunnerServiceRolePolicy

Descrição: permite que RoboRunner a AWS IoT gerencie AWS os recursos associados em nome do cliente.

`AWSIotRoboRunnerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 21 de fevereiro de 2023, 16:56 UTC
- Hora da edição: 21 de fevereiro de 2023, 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIotRoboRunnerServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
```

```
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/Usage"
        ]
      }
    }
  }
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTRuleActions

Descrição: Permite o acesso a todos os AWS serviços suportados nas ações de regras de AWS IoT

`AWSIoTRuleActions` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTRuleActions` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 08 de outubro de 2015, 15:14 UTC
- Hora da edição: 16 de janeiro de 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "dynamodb:PutItem",
      "kinesis:PutRecord",
      "iot:Publish",
      "s3:PutObject",
      "sns:Publish",
      "sqs:SendMessage*",
      "cloudwatch:SetAlarmState",
      "cloudwatch:PutMetricData",
      "es:ESHttpPut",
      "firehose:PutRecord"
    ],
    "Resource" : "*"
  }
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTSiteWiseConsoleFullAccess

Descrição: Fornece acesso total para gerenciar a AWS IoT SiteWise usando o. Console de gerenciamento da AWS Observe que essa política também concede acesso para criar e listar armazenamentos de dados usados com AWS IoT SiteWise (por exemplo, AWS IoT Analytics), acesso para listar e visualizar recursos do AWS IoT Greengrass, listar e modificar AWS segredos do Secrets Manager, recuperar sombras da AWS IoT, listar recursos com tags específicas e criar e usar uma função vinculada a serviços para IoT. AWS SiteWise

`AWSIoTSiteWiseConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTSiteWiseConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 31 de maio de 2019, 21:37 UTC
- Hora da edição: 31 de maio de 2019, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "iotsitewise:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iotanalytics:List*",
        "iotanalytics:Describe*",
        "iotanalytics:Create*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
```

```
        "iot:DescribeEndpoint",
        "iot:GetThingShadow"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:ListGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "secretsmanager:ListSecrets",
        "secretsmanager:CreateSecret"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "secretsmanager:UpdateSecret"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
    },
    {
      "Action" : [
        "tag:GetResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "iotsitewise.amazonaws.com"
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "iotsitewise.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTSiteWiseFullAccess

Descrição: Fornece acesso total à IoT. SiteWise

`AWSIoTSiteWiseFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTSiteWiseFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 04 de dezembro de 2018, 20:53 UTC
- Hora da edição: 04 de dezembro de 2018, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTSiteWiseMonitorPortalAccess

Descrição: Essa política concede permissões para acessar SiteWise ativos e dados de ativos de AWS IoT, criar recursos do AWS IoT SiteWise Monitor e listar usuários de AWS SSO.

`AWSIoTSiteWiseMonitorPortalAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTSiteWiseMonitorPortalAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 19 de maio de 2020, 20:01 UTC
- Hora da edição: 19 de maio de 2020, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:CreateProject",
```

```
        "iotsitewise:DescribeProject",
        "iotsitewise:UpdateProject",
        "iotsitewise:DeleteProject",
        "iotsitewise:ListProjects",
        "iotsitewise:BatchAssociateProjectAssets",
        "iotsitewise:BatchDisassociateProjectAssets",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:CreateDashboard",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:UpdateDashboard",
        "iotsitewise:DeleteDashboard",
        "iotsitewise:ListDashboards",
        "iotsitewise:CreateAccessPolicy",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:UpdateAccessPolicy",
        "iotsitewise:DeleteAccessPolicy",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:DescribeAsset",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetAssetPropertyAggregates",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTSiteWiseMonitorServiceRolePolicy

Descrição: Essa função concede ao SiteWise monitor de AWS IoT permissões para acessar seus ativos e propriedades de SiteWise ativos de AWS IoT e criar projetos, painéis e políticas de acesso do AWS IoT Sitewise por meio de portais de IoT. AWS SiteWise

`AWSIoTSiteWiseMonitorServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 14 de novembro de 2019, 0:59 UTC
- Hora da edição: 13 de dezembro de 2019, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:CreateProject",
```

```
        "iotsitewise:DescribeProject",
        "iotsitewise:UpdateProject",
        "iotsitewise:DeleteProject",
        "iotsitewise:ListProjects",
        "iotsitewise:BatchAssociateProjectAssets",
        "iotsitewise:BatchDisassociateProjectAssets",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:CreateDashboard",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:UpdateDashboard",
        "iotsitewise:DeleteDashboard",
        "iotsitewise:ListDashboards",
        "iotsitewise:CreateAccessPolicy",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:UpdateAccessPolicy",
        "iotsitewise:DeleteAccessPolicy",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:DescribeAsset",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetAssetPropertyAggregates",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTSiteWiseReadOnlyAccess

Descrição: Fornece acesso somente para leitura à IoT. SiteWise

`AWSIoTSiteWiseReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTSiteWiseReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 04 de dezembro de 2018, 20:55 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:BatchGetAssetPropertyAggregates",
        "iotsitewise:BatchGetAssetPropertyValue",
        "iotsitewise:BatchGetAssetPropertyValueHistory",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAction",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetCompositeModel",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeAssetModelCompositeModel",
        "iotsitewise:DescribeAssetModelInterfaceRelationship",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:DescribeBulkImportJob",
        "iotsitewise:DescribeComputationModel",
```

```
        "iotsitewise:DescribeComputationModelExecutionSummary",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeDataset",
        "iotsitewise:DescribeDefaultEncryptionConfiguration",
        "iotsitewise:DescribeExecution",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribeGatewayCapabilityConfiguration",
        "iotsitewise:DescribeLoggingOptions",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:DescribeStorageConfiguration",
        "iotsitewise:DescribeTimeSeries",
        "iotsitewise:ExecuteQuery",
        "iotsitewise:GetAssetPropertyAggregates",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetInterpolatedAssetPropertyValues",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListActions",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssetRelationships",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListBulkImportJobs",
        "iotsitewise:ListCompositionRelationships",
        "iotsitewise:ListComputationModelDataBindingUsages",
        "iotsitewise:ListComputationModelResolveToResources",
        "iotsitewise:ListComputationModels",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "iotsitewise:ListExecutions",
        "iotsitewise:ListGateways",
        "iotsitewise:ListInterfaceRelationships",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iotsitewise:ListTimeSeries"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTThingsRegistration

Descrição: Essa política permite que os usuários registrem itens em massa usando a API de AWS IoT StartThingRegistrationTask

`AWSIoTThingsRegistration` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTThingsRegistration` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 01 de dezembro de 2017, 20:21 UTC
- Hora da edição: 05 de outubro de 2020, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:AddThingToThingGroup",
        "iot:AttachPolicy",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CreateCertificateFromCsr",
        "iot:CreatePolicy",
        "iot:CreateThing",
        "iot:DescribeCertificate",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:DetachPolicy",
        "iot:DetachThingPrincipal",
        "iot:GetPolicy",
        "iot:ListAttachedPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:RegisterCertificate",
        "iot:RegisterThing",
        "iot:RemoveThingFromThingGroup",
        "iot:UpdateCertificate",
        "iot:UpdateThing",
        "iot:UpdateThingGroupsForThing",
        "iot:AddThingToBillingGroup",
        "iot:DescribeBillingGroup",
        "iot:RemoveThingFromBillingGroup"
      ],
      "Resource" : [
        "*"
      ]
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTTwinMakerServiceRolePolicy

Descrição: permite que TwinMaker a AWS IoT ligue para outros AWS serviços e sincronize seus recursos em seu nome.

`AWSIoTTwinMakerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 13 de novembro de 2023, 18:59 UTC
- Hora da edição: 13 de novembro de 2023, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTTwinMakerServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SiteWiseAssetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAsset"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset/*"
      ]
    },
    {
      "Sid" : "SiteWiseAssetModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAssetModel"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset-model/*"
      ]
    },
    {
      "Sid" : "SiteWiseAssetModelAndAssetListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssetModels"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TwinMakerAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iottwinmaker:GetEntity",
        "iottwinmaker:CreateEntity",
        "iottwinmaker:UpdateEntity",
        "iottwinmaker:DeleteEntity",
        "iottwinmaker:ListEntities",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:CreateComponentType",
        "iottwinmaker:UpdateComponentType",
        "iottwinmaker:DeleteComponentType",
        "iottwinmaker:ListComponentTypes"
      ],
      "Resource" : [
        "arn:aws:iottwinmaker:*:*:workspace/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITEWISE"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTWirelessDataAccess

Descrição: Permite que os dados de identidade associados acessem dispositivos AWS IoT Wireless.

`AWSIoTWirelessDataAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTWirelessDataAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de dezembro de 2020, 15:31 UTC
- Hora da edição: 15 de dezembro de 2020, 15:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotwireless:SendDataToWirelessDevice"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTWirelessFullAccess

Descrição: permite que a identidade associada tenha acesso total a todas as operações AWS do IoT Wireless.

`AWSIoTWirelessFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTWirelessFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de dezembro de 2020, 15:27 UTC
- Hora da edição: 15 de dezembro de 2020, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotwireless:*"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTWirelessFullPublishAccess

Descrição: fornece ao IoT Wireless acesso total para publicar no IoT Rules Engine em seu nome.

`AWSIoTWirelessFullPublishAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTWirelessFullPublishAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de dezembro de 2020, 15:29 UTC
- Hora da edição: 15 de dezembro de 2020, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint",
        "iot:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTWirelessGatewayCertManager

Descrição: permite o acesso à identidade associada para criar, listar e descrever certificados de IoT

`AWSIoTWirelessGatewayCertManager` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTWirelessGatewayCertManager` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de dezembro de 2020, 15:30 UTC
- Hora da edição: 15 de dezembro de 2020, 15:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTWirelessLogging

Descrição: permite que a identidade associada crie grupos do Amazon CloudWatch Logs e transmita registros para os grupos.

`AWSIoTWirelessLogging` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTWirelessLogging` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de dezembro de 2020, 15:32 UTC
- Hora da edição: 15 de dezembro de 2020, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessLogging`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotwireless*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIoTWirelessReadOnlyAccess

Descrição: Permite que a identidade associada tenha acesso somente para leitura à AWS IoT sem fio.

`AWSIoTWirelessReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIoTWirelessReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de dezembro de 2020, 15:28 UTC
- Hora da edição: 15 de dezembro de 2020, 15:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotwireless:List*",
        "iotwireless:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIPAMServiceRolePolicy

Descrição: permite que o VPC IP Address Manager acesse os recursos da VPC e se integre às AWS organizações em seu nome.

`AWSIPAMServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 30 de novembro de 2021, 19:08 UTC
- Horário editado: 09 de setembro de 2026, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IPAMDiscoveryDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "ec2:GetIpamDiscoveredRoutes",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListByoipCidrs",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit",
        "cloudfront:ListAnycastIpLists",
        "cloudfront:ListDistributionsByAnycastIpListId",
```

```
        "cloudfront:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchMetricsPublishActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/IPAM"
        }
      }
    },
    {
      "Sid" : "IPAMAllocationPolicyActions",
      "Effect" : "Allow",
      "Action" : "ec2:AllocateIpamPoolCidr",
      "Resource" : "*"
    },
    {
      "Sid" : "PrefixListResolverWriteActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyManagedPrefixList"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:Attribute/ExpectedIpamPrefixListResolverTarget" : "false"
        }
      }
    },
    {
      "Sid" : "PrefixListResolverReadActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : [
```

```
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIQContractServiceRolePolicy

Descrição: Usado pela AWS IQ para executar solicitações de pagamento em nome de um cliente

`AWSIQContractServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 22 de agosto de 2019, 19:28 UTC
- Hora da edição: 22 de agosto de 2019, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:Subscribe"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIQFullAccess

Descrição: Fornece acesso total ao AWS QI

`AWSIQFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSIQFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 04 de abril de 2019, 23:13 UTC
- Hora da edição: 25 de setembro de 2019, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIQFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iq:*",
        "iq-permission:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "permission.iq.amazonaws.com",
            "contract.iq.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSIQPermissionServiceRolePolicy

Descrição: Permite que o AWS IQ gerencie a função assumida pelos especialistas em AWS QI.

`AWSIQPermissionServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 22 de agosto de 2019, 19:36 UTC
- Hora da edição: 22 de agosto de 2019, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSDenyAll"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

Descrição: Permite o acesso aos AWS serviços e recursos necessários para armazenamentos de chaves personalizadas do AWS KMS

`AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 14 de novembro de 2018, 20:10 UTC
- Hora da edição: 10 de novembro de 2023, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
```

```
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

Descrição: permite que o AWS KMS sincronize as propriedades compartilhadas das chaves multirregionais.

`AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 16 de junho de 2021, 15:37 UTC
- Horário editado: 13 de novembro de 2024, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KMSSynchronizeMultiRegionKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:SynchronizeMultiRegionKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSKeyManagementServicePowerUser

Descrição: Fornece acesso ao Serviço de Gerenciamento de AWS Chaves (KMS).

`AWSKeyManagementServicePowerUser` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSKeyManagementServicePowerUser` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC

- Hora da edição: 7 de março de 2017, 0:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms:DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
        "kms:TagResource",
        "kms:UntagResource",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLakeFormationCrossAccountManager

Descrição: fornece acesso entre contas aos recursos do Glue via Lake Formation. Também concede acesso de leitura a outros serviços necessários, como organizações e gerenciador de acesso a recursos

`AWSLakeFormationCrossAccountManager` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLakeFormationCrossAccountManager` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 04 de agosto de 2020, 20:59 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "AllowCreateResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManageResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManageResourceSharePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceSharePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
```

```
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowXAcctManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:PutResourcePolicy",
        "glue:DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "ram:Get*",
        "ram:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLakeFormationDataAdmin

Descrição: Concede acesso administrativo ao AWS Lake Formation e aos serviços relacionados, como o AWS Glue, para gerenciar data lakes

`AWSLakeFormationDataAdmin` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLakeFormationDataAdmin` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de agosto de 2019, 17:33 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLakeFormationDataAdminAllow",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "glue:CreateCatalog",
        "glue:UpdateCatalog",
```

```
        "glue:DeleteCatalog",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:GetConnections",
        "glue:SearchTables",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:GetTableVersions",
        "glue:GetPartitions",
        "glue:GetTables",
        "glue:ListWorkflows",
        "glue:BatchGetWorkflows",
        "glue:DeleteWorkflow",
        "glue:GetWorkflowRuns",
        "glue:StartWorkflowRun",
        "glue:GetWorkflow",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "iam:ListUsers",
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSLakeFormationDataAdminDeny",
      "Effect" : "Deny",
      "Action" : [
        "lakeformation:PutDataLakeSettings"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWS Lambda_FullAccess

Descrição: concede acesso total ao serviço AWS Lambda, aos recursos do console AWS Lambda e a outros serviços relacionados AWS .

`AWSLambda_FullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLambda_FullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de novembro de 2020, 21:14 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_FullAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "lambda:*",
        "logs:DescribeLogGroups",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lambda.amazonaws.com/
AWSServiceRoleForLambda",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWS Lambda_ReadOnlyAccess

Descrição: concede acesso somente para leitura ao serviço AWS Lambda, aos recursos do console AWS Lambda e a outros serviços relacionados. AWS

`AWSLambda_ReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLambda_ReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de novembro de 2020, 21:10 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
```

```
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "lambda:Get*",
        "lambda:List*",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:DescribeQueries",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:GetQueryResults",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLambdaBasicDurableExecutionRolePolicy

Descrição: fornece permissões de gravação para CloudWatch registros e read/write permissões para APIs de execução durável usadas pelas funções duráveis do Lambda

`AWSLambdaBasicDurableExecutionRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLambdaBasicDurableExecutionRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 02 de dezembro de 2025, 15:04 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicDurableExecutionRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
```

```
        "logs:PutLogEvents",
        "lambda:CheckpointDurableExecution",
        "lambda:GetDurableExecutionState"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLambdaBasicExecutionRole

Descrição: Fornece permissões de gravação em CloudWatch registros.

`AWSLambdaBasicExecutionRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLambdaBasicExecutionRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 09 de abril de 2015, 15:03 UTC
- Hora da edição: 09 de abril de 2015, 15:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLambdaDynamoDBExecutionRole

Descrição: Fornece acesso de lista e leitura aos streams do DynamoDB e permissões de gravação nos registros. CloudWatch

`AWSLambdaDynamoDBExecutionRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLambdaDynamoDBExecutionRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 09 de abril de 2015, 15:09 UTC
- Hora da edição: 09 de abril de 2015, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLambdaENIManagementAccess

Descrição: fornece permissões mínimas para uma função do Lambda gerenciar ENIs (criar, descrever, excluir) usados por uma função do VPC-enabled Lambda.

`AWSLambdaENIManagementAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLambdaENIManagementAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 6 de dezembro de 2016, 0:37 UTC
- Hora da edição: 01 de outubro de 2020, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLambdaExecute

> **Important**
>
> A política `AWSLambdaExecute` gerenciada está prestes a ser descontinuada e não é mais recomendada para uso com o AWS Lambda. Em seu lugar, use `AWSLambdaBasicExecutionRole`. Quando o serviço IAM eventualmente descontinuar a política, você não poderá anexá-la a uma função. No entanto, você pode anexar uma função existente a um recurso, mesmo que essa função use a política obsoleta.

Descrição: Fornece Put, Get acesso ao S3 e acesso total aos CloudWatch Logs.

`AWSLambdaExecute` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLambdaExecute` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaExecute`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLambdaFullAccess

Descrição: esta política será descontinuada. Consulte a documentação para obter orientação: https://docs.aws.amazon.com/lambda/latest/dg/access-control-identity-based.html. Fornece acesso total ao Lambda, S3, DynamoDB, CloudWatch Metrics and Logs.

`AWSLambdaFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLambdaFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 27 de novembro de 2017, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaFullAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudwatch:*",
        "cognito-identity:ListIdentityPools",
        "cognito-sync:GetCognitoEvents",
        "cognito-sync:SetCognitoEvents",
        "dynamodb:*",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "events:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:PassRole",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy",
        "iot:CreateThing",
        "iot:CreateTopicRule",
        "iot:DescribeEndpoint",
        "iot:GetTopicRule",
        "iot:ListPolicies",
        "iot:ListThings",
        "iot:ListTopicRules",
        "iot:ReplaceTopicRule",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kms:ListAliases",
        "lambda:*",
```

```
        "logs:*",
        "s3:*",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Publish",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sqs:ListQueues",
        "sqs:SendMessage",
        "tag:GetResources",
        "xray:PutTelemetryRecords",
        "xray:PutTraceSegments"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLambdaInvocation-DynamoDB

Descrição: fornece acesso de leitura ao DynamoDB Streams.

`AWSLambdaInvocation-DynamoDB` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLambdaInvocation-DynamoDB` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLambdaInvokeWebFunctionEndpointAccess

Descrição: Concede permissão para invocar os endpoints da função Web do AWS Lambda.

`AWSLambdaInvokeWebFunctionEndpointAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLambdaInvokeWebFunctionEndpointAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 01 de outubro de 2026, 16:47 UTC
- Horário editado: 01 de outubro de 2026, 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvokeWebFunctionEndpointAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "lambda:InvokeWebFunctionEndpoint"
      ],
      "Resource" : "arn:aws:lambda:*:*:web-function/*/endpoint/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLambdaKinesisExecutionRole

Descrição: fornece acesso de lista e leitura aos streams do Kinesis e permissões de gravação nos registros. CloudWatch

`AWSLambdaKinesisExecutionRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLambdaKinesisExecutionRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 09 de abril de 2015, 15:14 UTC
- Hora da edição: 19 de novembro de 2018, 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetRecords",
        "kinesis:GetShardIterator",
        "kinesis:ListShards",
        "kinesis:ListStreams",
        "kinesis:SubscribeToShard",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLambdaManagedEC2ResourceOperator

Descrição: Essa política concede permissões para criar e administrar recursos do EC2 gerenciados pelas instâncias gerenciadas do Lambda e permissões descritivas.

`AWSLambdaManagedEC2ResourceOperator` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLambdaManagedEC2ResourceOperator` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 30 de novembro de 2025, 08:34 UTC
- Horário editado: 10 de junho de 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaManagedEC2ResourceOperator`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateTags",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "scaler.lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEncryptionControls"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : "amazon"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*:log-stream:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLambdaMSKExecutionRole

Descrição: fornece as permissões necessárias para acessar o MSK Cluster em uma VPC, gerenciar ENIs (criar, descrever, excluir) na VPC e gravar permissões nos registros. CloudWatch

`AWSLambdaMSKExecutionRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLambdaMSKExecutionRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço

- Hora da criação: 11 de agosto de 2020, 17:35 UTC
- Hora da edição: 02 de agosto de 2022, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:GetBootstrapBrokers",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLambdaNetworkConnectorOperatorPolicy

Descrição: Essa política concede permissões para criar e administrar recursos ENI gerenciados pelo Lambda Network Connector.

`AWSLambdaNetworkConnectorOperatorPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLambdaNetworkConnectorOperatorPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 22 de junho de 2026, 15:27 UTC
- Horário editado: 22 de junho de 2026, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaNetworkConnectorOperatorPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateEniInAnySubnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
    },
    {
      "Sid" : "AllowCreateEniWithSecurityGroups",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "AllowCreateEniWithLambdaTagKeys",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:lambda:networkConnectorName",
            "aws:lambda:networkConnectorId"
          ]
        }
      }
    },
    {
      "Sid" : "TagENIOnCreate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface",
          "ec2:ManagedResourceOperator" : "network-connectors.lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLambdaReplicator

Descrição: concede ao Lambda Replicator as permissões necessárias para replicar funções em todas as regiões

`AWSLambdaReplicator` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 23 de maio de 2017, 17:53 UTC
- Hora da edição: 08 de dezembro de 2017, 0:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LambdaCreateDeletePermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:DisableReplication"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "IamPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFrontListDistributions",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionsByLambdaFunction"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLambdaRole

Descrição: política padrão para a função de serviço do AWS Lambda.

`AWSLambdaRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLambdaRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaRole`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLambdaServiceRolePolicy

Descrição: permite que o Lambda descreva e encerre instâncias gerenciadas do EC2 em seu nome.

`AWSLambdaServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Tempo de criação: 30 de novembro de 2025, 08:04 UTC
- Horário editado: 22 de junho de 2026, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "scaler.lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "network-connectors.lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLambdaSQSQueueExecutionRole

Descrição: fornece acesso a mensagens de recebimento, exclusão de mensagens e atributos de leitura às filas SQS e permissões de gravação em registros. CloudWatch

`AWSLambdaSQSQueueExecutionRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLambdaSQSQueueExecutionRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 14 de junho de 2018, 21:50 UTC
- Hora da edição: 14 de junho de 2018, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLambdaVPCAccessExecutionRole

Descrição: fornece permissões mínimas para que uma função do Lambda seja executada ao acessar um recurso em uma VPC — crie, descreva, exclua interfaces de rede e grave permissões em registros. CloudWatch

`AWSLambdaVPCAccessExecutionRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLambdaVPCAccessExecutionRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 11 de fevereiro de 2016, 23:15 UTC
- Hora da edição: 5 de janeiro de 2024, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLambdaVPCAccessExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
```

```
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLicenseManagerConsumptionPolicy

Descrição: fornece permissões para permitir o acesso às ações da API do AWS License Manager que devem ser consumidas com base nas licenças às quais o usuário tem direitos.

`AWSLicenseManagerConsumptionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSLicenseManagerConsumptionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 11 de agosto de 2021, 23:18 UTC
- Hora da edição: 11 de agosto de 2021, 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

Descrição: permite que o AWS License Manager Linux Subscriptions Service gerencie recursos em seu nome.

`AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 20 de dezembro de 2022, 18:54 UTC
- Hora da edição: 8 de julho de 2024, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LicenseManagerLinuxSubscriptions" : "enabled",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*"
      ]
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LicenseManagerLinuxSubscriptions" : "enabled",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLicenseManagerMasterAccountRolePolicy

Descrição: Política de função da conta principal do serviço AWS License Manager

`AWSLicenseManagerMasterAccountRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 26 de novembro de 2018, 19:03 UTC
- Hora da edição: 31 de maio de 2022, 20:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
```

```
      "Sid" : "S3ObjectPermissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*/resource_sync/*"
      ]
    },
    {
      "Sid" : "AthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "GluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTable",
        "glue:GetPartition",
        "glue:GetPartitions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
```

```
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RAMPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareAssociations",
        "ram:TagResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RAMPermissions2",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Service" : "LicenseManager"
        }
      }
    },
    {
      "Sid" : "RAMPermissions3",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Service" : "LicenseManager"
        }
      }
    },
    {
      "Sid" : "IAMGetRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMPassRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/LicenseManagerServiceResourceDataSyncRole*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "cloudformation.amazonaws.com",
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudformationPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks"
      ],
```

```
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/
LicenseManagerCrossAccountCloudDiscoveryStack/*"
      ]
    },
    {
      "Sid" : "GlueUpdatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:UpdateJob",
        "glue:UpdateCrawler"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:crawler/LicenseManagerResourceSynDataCrawler",
        "arn:aws:glue:*:*:job/LicenseManagerResourceSynDataProcessJob",
        "arn:aws:glue:*:*:table/license_manager_resource_inventory_db/*",
        "arn:aws:glue:*:*:table/license_manager_resource_sync/*",
        "arn:aws:glue:*:*:database/license_manager_resource_inventory_db",
        "arn:aws:glue:*:*:database/license_manager_resource_sync"
      ]
    },
    {
      "Sid" : "RGPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:PutGroupPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLicenseManagerMemberAccountRolePolicy

Descrição: Política de função da conta de membro do serviço do AWS License Manager

`AWSLicenseManagerMemberAccountRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 26 de novembro de 2018, 19:04 UTC
- Hora da edição: 15 de novembro de 2019, 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "LicenseManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:GetLicenseConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListInventoryEntries",
        "ssm:GetInventory",
        "ssm:CreateAssociation",
        "ssm:CreateResourceDataSync",
        "ssm:DeleteResourceDataSync",
        "ssm:ListResourceDataSync",
        "ssm:ListAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RAMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLicenseManagerServiceRolePolicy

Descrição: Política de função padrão do serviço AWS License Manager

`AWSLicenseManagerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 26 de novembro de 2018, 19:02 UTC
- Horário editado: 19 de novembro de 2025, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "IAMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/license-
management.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManagement"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "license-management.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPermissionsForCreatingMemberSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/license-manager.member-
account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "license-manager.member-account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3BucketPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
```

```
      "Sid" : "S3BucketPermissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "SNSAccountPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "SNSTopicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
```

```
        "ec2:DescribeImages",
        "ec2:DescribeHosts"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListInventoryEntries",
        "ssm:GetInventory",
        "ssm:CreateAssociation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMSendCommandPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*::document/AWSLicenseManager-*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "LicenseManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "license-manager:GetServiceSettings",
        "license-manager:GetLicense*",
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

Descrição: Permite que o Serviço de Assinaturas de Usuários do AWS License Manager gerencie recursos em seu nome.

`AWSLicenseManagerUserSubscriptionsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 30 de julho de 2022, 1:17 UTC
- Horário editado: 10 de julho de 2026, 20:42 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:GetAuthorizedApplicationDetails",
        "ds:DescribeTrusts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetInventory",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
```

```
        "ec2:DescribeVpcPeeringConnections"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2WritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:productCode" : [
            "bz0vcy31ooqlzk5tsash4r1ik",
            "d44g89hc0gp9jdzm99rznthpw",
            "77yzkpa7kvee1y1tt7wnsdwoc",
            "a8jthu9h8pjsn4b8ylvfl6sfr",
            "7at6der8hnlov1g347e6tdkde",
            "3t0v0vuhvxjzm6m462f9v8iz4",
            "4gs2prcp03ojilgkjx8m3ifh7",
            "5uypd9kpy863kwykrwn4bcolv",
            "eqtok9gt75we12qgk28b955qc"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "SSMDocumentExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunPowerShellScript"
      ]
    },
    {
      "Sid" : "SSMInstanceExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSLicenseManager" : "UserSubscriptions"
        }
      }
    },
    {
      "Sid" : "ReadHostedZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListResourceRecordSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadSecurityGroupRulePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupRules"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Sid" : "DescribeSubnetsPermissions",
      "Action" : [
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeNetworkInterfacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "DescribeVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadSecretPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:license-manager-user-*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSM2ServicePolicy

Descrição: Permite que o AWS M2 gerencie AWS recursos em seu nome.

`AWSM2ServicePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 07 de junho de 2022, 20:26 UTC

- Hora da edição: 07 de junho de 2022, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/M2"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSManagedAccountManagementAccess

Descrição: Concede AWS permissões para atualizar e manter funções AWS gerenciadas para contas AWS gerenciadas

`AWSManagedAccountManagementAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSManagedAccountManagementAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 20 de julho de 2026, 19:57 UTC
- Horário editado: 01 de outubro de 2026, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedAccountManagementAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:TagRole",
        "iam:UntagRole",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole"
      ],
      "Resource" : "arn:*:iam::*:role/managed/*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:*:iam::*:role/managed/AWSManagedAccountManagementAccessRole",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSManagedAccountUserEntitlementAccess

Descrição: Concede AWS permissões para gerenciar direitos de acesso à conta para AWS contas gerenciadas

`AWSManagedAccountUserEntitlementAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSManagedAccountUserEntitlementAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 17 de julho de 2026, 21:42 UTC
- Horário editado: 17 de julho de 2026, 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedAccountUserEntitlementAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "identitystore:CreateGroup",
      "identitystore:GetGroupId",
      "identitystore:GetUserId",
      "identitystore:CreateGroupMembership",
      "sso:ListInstances",
      "sso-directory:ListProvisioningTenants",
      "account-access:ListApplications",
      "account-access:CreateEntitlement",
      "account-access:ListEntitlements"
    ],
    "Resource" : "*"
  }
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSManagedAdvancedFeaturesActivationAccess

Descrição: Concede AWS permissão para ativar recursos avançados para contas AWS gerenciadas

`AWSManagedAdvancedFeaturesActivationAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSManagedAdvancedFeaturesActivationAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 21 de julho de 2026, 14:27 UTC
- Horário editado: 21 de julho de 2026, 14:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedAdvancedFeaturesActivationAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "iam:PutAccountProperties"
    ],
    "Resource" : "*"
  }
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSManagedBudgetsSpendLimitManagementAccess

Descrição: Concede ao serviço de AWS orçamentos permissões para anexar e desanexar políticas de controle de serviços e gerenciar contas em uma AWS organização para impor limites de gastos nas contas dos membros.

`AWSManagedBudgetsSpendLimitManagementAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSManagedBudgetsSpendLimitManagementAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 17 de julho de 2026, 21:12 UTC
- Horário editado: 07 de agosto de 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedBudgetsSpendLimitManagementAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "SCPActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:AttachPolicy",
        "organizations:DescribePolicy",
        "organizations:DetachPolicy"
      ],
      "Resource" : "arn:aws:organizations::*:policy/*/service_control_policy/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedBy" : "SpendLimit"
        }
      }
    },
    {
      "Sid" : "SCPListPolicyAction",
      "Effect" : "Allow",
      "Action" : "organizations:ListPolicies",
      "Resource" : "*"
    },
    {
      "Sid" : "SCPTargetActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:AttachPolicy",
        "organizations:DetachPolicy"
      ],
      "Resource" : "arn:aws:organizations::*:account/*"
    },
    {
      "Sid" : "AccountActions",
      "Effect" : "Allow",
      "Action" : "organizations:CloseAccount",
      "Resource" : "arn:aws:organizations::*:account/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSManagedControlPolicyManagementAccess

Descrição: Concede AWS permissão para gerenciar políticas de controle organizacional para contas AWS gerenciadas

`AWSManagedControlPolicyManagementAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSManagedControlPolicyManagementAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 21 de julho de 2026, 14:27 UTC
- Horário editado: 21 de julho de 2026, 14:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedControlPolicyManagementAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribePolicy",
```

```
      "organizations:UpdatePolicy",
      "organizations:ListPolicies",
      "organizations:ListRoots",
      "organizations:CreatePolicy",
      "organizations:AttachPolicy",
      "organizations:DetachPolicy",
      "organizations:DeletePolicy",
      "organizations:TagResource",
      "organizations:UntagResource",
      "organizations:ListTagsForResource"
    ],
    "Resource" : "*"
  }
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSManagedServiceAccessManagementAccess

Descrição: Concede permissões para gerenciar políticas de controle de serviços (SCPs) em AWS organizações para o serviço de gerenciamento de acesso a serviços AWS gerenciados. Inclui permissões para listar, criar, atualizar e anexar SCPs com escopo a políticas marcadas com ManagedBy =service-access.

`AWSManagedServiceAccessManagementAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSManagedServiceAccessManagementAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço

- Horário de criação: 21 de julho de 2026, 17:57 UTC
- Horário editado: 21 de julho de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSManagedServiceAccessManagementAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowListRoots",
      "Effect" : "Allow",
      "Action" : "organizations:ListRoots",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSCPList",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : "SERVICE_CONTROL_POLICY"
        }
      }
    },
    {
      "Sid" : "AllowSCPCreateWithTag",
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:CreatePolicy",
        "organizations:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : "SERVICE_CONTROL_POLICY",
          "aws:RequestTag/ManagedBy" : "service-access"
        }
      }
    },
    {
      "Sid" : "AllowSCPUpdateTagged",
      "Effect" : "Allow",
      "Action" : "organizations:UpdatePolicy",
      "Resource" : "arn:aws:organizations::*:policy/*/service_control_policy/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedBy" : "service-access"
        }
      }
    },
    {
      "Sid" : "AllowSCPAttachTaggedPolicy",
      "Effect" : "Allow",
      "Action" : "organizations:AttachPolicy",
      "Resource" : "arn:aws:organizations::*:policy/*/service_control_policy/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedBy" : "service-access"
        }
      }
    },
    {
      "Sid" : "AllowSCPAttachRoot",
      "Effect" : "Allow",
      "Action" : "organizations:AttachPolicy",
      "Resource" : "arn:aws:organizations::*:root/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSManagedServices_ContactsServiceRolePolicy

Descrição: permite que os serviços AWS gerenciados leiam os valores das tags nos AWS recursos

`AWSManagedServices_ContactsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 23 de março de 2023, 17:07 UTC
- Hora da edição: 23 de março de 2023, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoleTags",
        "iam:ListUserTags",
        "tag:GetResources",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetBucketTagging",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:authType" : "REST-HEADER",
          "s3:signatureversion" : "AWS4-HMAC-SHA256"
        },
        "NumericGreaterThanEquals" : {
          "s3:TlsVersion" : "1.2"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

Descrição: Serviços AWS gerenciados — política para gerenciar a infraestrutura de controles de detetives

`AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 19 de dezembro de 2022, 23:11 UTC
- Hora da edição: 19 de dezembro de 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateTermination*",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackResources",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
```

```
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-config-recorder",
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-config-rules-cdk",
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-infrastructure-cdk"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeAggregationAuthorizations",
        "config:PutAggregationAuthorization",
        "config:TagResource",
        "config:PutConfigRule"
      ],
      "Resource" : [
        "arn:aws:config:*:*:aggregation-authorization/540708452589/*",
        "arn:aws:config:*:*::config-rule/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy",
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetBucketAcl",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketLogging",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::ams-config-record-bucket-*"
```

```
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSManagedServices_EventsServiceRolePolicy

Descrição: Política de serviços AWS gerenciados para ativar o recurso de processador de eventos AMS.

`AWSManagedServices_EventsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 07 de fevereiro de 2023, 18:41 UTC
- Hora da edição: 07 de fevereiro de 2023, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "events.managedservices.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSManagedServices_SelfServiceReporting_ServiceRolePolicy

Descrição: permite que o recurso de relatórios de autoatendimento do Serviço AWS Gerenciado da Amazon leia os dados AWS da organização em seu nome para permitir relatórios agregados em nível organizacional

`AWSManagedServices_SelfServiceReporting_ServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 08 de janeiro de 2025, 21:22 UTC
- Horário editado: 08 de janeiro de 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_SelfServiceReporting_ServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSManagedServicesDeploymentToolkitPolicy

Descrição: permite que o AWS Managed Services gerencie o kit de ferramentas de implantação em seu nome.

`AWSManagedServicesDeploymentToolkitPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 09 de junho de 2022, 18:33 UTC
- Hora da edição: 4 de abril de 2024, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AMSCDKToolkitS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObject",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersion",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketVersioning",
        "s3:GetLifecycleConfiguration",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectAttributes",
        "s3:GetObjectLegalHold",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionAttributes",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionTorrent",
        "s3:ListBucket",
        "s3:ListBucketVersions",
```

```
        "s3:PutBucketAcl",
        "s3:PutBucketLogging",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::ams-cdktoolkit*"
    },
    {
      "Sid" : "AMSCDKToolkitCloudFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:GetTemplateSummary",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:UpdateTerminationProtection"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*"
    },
    {
      "Sid" : "AMSCDKToolkitECRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:CreateRepository",
        "ecr:DeleteLifecyclePolicy",
        "ecr:DeleteRepository",
        "ecr:DeleteRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:ListTagsForResource",
```

```
        "ecr:PutImageScanningConfiguration",
        "ecr:PutImageTagMutability",
        "ecr:PutLifecyclePolicy",
        "ecr:SetRepositoryPolicy",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/ams-cdktoolkit*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSManagedSettingsAdminAccess

Descrição: Concede acesso administrativo total ao gerenciamento de Conta da AWS configurações. Essa política permite que os proprietários visualizem e modifiquem informações da conta, faturamento, pagamentos, registro fiscal, gerenciamento de identidade, políticas da organização, orçamentos, análise de custos e notificações do espaço de trabalho. Destinado a proprietários de workspaces que precisam de acesso administrativo completo sobre a configuração da conta e o gerenciamento de membros. A política não concede acesso a serviços de computação, armazenamento, rede ou outros serviços de infraestrutura não relacionados às configurações da conta.

`AWSManagedSettingsAdminAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSManagedSettingsAdminAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 22 de julho de 2026, 01:27 UTC
- Horário editado: 30 de setembro de 2026, 22:27 UTC

- ARN: `arn:aws:iam::aws:policy/AWSManagedSettingsAdminAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ActivateAdvancedUpdateAccountName",
      "Effect" : "Allow",
      "Action" : [
        "account:PutAccountName"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSettingsAccountAccess",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetContactInformation",
        "account:CloseAccount",
        "account:PutAccountName",
        "account:PutContactInformation",
        "account:StartPrimaryEmailUpdate",
        "account:AcceptPrimaryEmailUpdate",
        "account:GetPrimaryEmailUpdateStatus",
        "account:SendPhoneNumberVerification",
        "account:VerifyPhoneNumber",
```

```
        "notifications:AssociateManagedNotificationAccountContact",
        "notifications:DisassociateManagedNotificationAccountContact",
        "notifications:ListManagedNotificationChannelAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsBillingAccess",
      "Effect" : "Allow",
      "Action" : [
        "billing:GetCredits",
        "billing:GetSellerOfRecord",
        "billing:RedeemCredits"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsCostExplorerAccess",
      "Effect" : "Allow",
      "Action" : [
        "ce:GetCostAndUsage",
        "ce:GetCostForecast"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsBudgetsAccess",
      "Effect" : "Allow",
      "Action" : [
        "budgets:CreateBudgetAction",
        "budgets:DeleteBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ModifyBudget",
        "budgets:ViewBudget",
        "budgets:UpdateBudget",
        "budgets:CreateBudget",
        "budgets:DeleteBudget",
        "budgets:DescribeBudgets",
        "budgets:DescribeBudget",
        "budgets:DescribeBudgetActionHistories"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AWSSettingsIAMPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/managed/
AWSManagedBudgetsSpendLimitManagementRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "budgets.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSettingsCustomerVerificationAccess",
      "Effect" : "Allow",
      "Action" : [
        "customer-verification:CreateCustomerVerificationDetails",
        "customer-verification:CreateUploadUrls",
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "customer-verification:UpdateCustomerVerificationDetails",
        "customer-verification:GetInheritanceConfig",
        "customer-verification:PutInheritanceConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsFreeTierAccess",
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState",
        "freetier:UpgradeAccountPlan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsIdentityStoreAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:CreateGroup",
        "identitystore:CreateGroupMembership",
        "identitystore:CreateUser",
        "identitystore:DeleteGroup",
        "identitystore:DeleteGroupMembership",
```

```
        "identitystore:DeleteUser",
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetUserId",
        "identitystore:ListGroupMemberships",
        "identitystore:UpdateIdentityStore",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
        "identitystore:ReserveUser",
        "identitystore:UpdateGroup",
        "identitystore:UpdateUser",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers",
        "builderid:CreateInvitation",
        "builderid:DeleteInvitation",
        "builderid:DisassociateCollaborator",
        "builderid:ListInvitations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsInvoicingAccess",
      "Effect" : "Allow",
      "Action" : [
        "invoicing:GetInvoicePDF"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:CloseAccount",
        "organizations:CreatePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:CreateBuilderIdOwnedAccount",
```

```
        "organizations:DescribeCreateAccountStatus",
        "organizations:DescribeAccount",
        "organizations:InviteAccountToOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsOrganizationsAiOptOutPolicyManagement",
      "Effect" : "Allow",
      "Action" : [
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : "AISERVICES_OPT_OUT_POLICY"
        }
      }
    },
    {
      "Sid" : "AWSSettingsPaymentsAccess",
      "Effect" : "Allow",
      "Action" : [
        "payments:CreatePaymentInstrument",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "payments:MakePayment",
        "payments:UpdatePaymentInstrument",
        "payments:UpdatePaymentPreferences",
        "payments:TagResource",
        "payments:UntagResource",
        "payments:ListTagsForResource",
        "payments:BatchGetPaymentProfiles",
        "payments:AcceptTermsAndConditionsForProgramByAccountId",
        "payments:CreatePaymentAttempt",
        "payments:CreatePaymentProfile",
        "payments:Get",
        "payments:GetAcceptedTermsAndConditionsForProgramByAccountId",
        "payments:GetEligibleCurrencies",
        "payments:GetPaymentAttempt",
```

```
        "payments:GetPaymentPreferences",
        "payments:GetPreferredCurrency",
        "payments:GetRecommendedTermsAndConditionsForProgram",
        "payments:ListPaymentProfiles",
        "payments:SearchFinancialRecords",
        "payments:SetPreferredCurrency",
        "payments:UpdatePaymentProfile",
        "payments:GetAccountBalance",
        "payments:GetDefaultPaymentProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsSESAccess",
      "Effect" : "Allow",
      "Action" : [
        "ses:SendEmail"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsSSOAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DeleteApplicationAssignment",
        "sso:DescribeInstance",
        "sso:GetApplicationAssignmentConfiguration",
        "sso:ListApplicationAssignments",
        "sso:CreateApplicationAssignment",
        "sso:DescribeApplication",
        "sso:ListApplications",
        "sso:UpdateInstance"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsTaxAccess",
      "Effect" : "Allow",
      "Action" : [
        "tax:BatchPutTaxRegistration",
        "tax:DeleteTaxRegistration",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
```

```
        "tax:PutTaxRegistration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSettingsSupportAccess",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeCases",
        "support:AddCommunicationToCase",
        "support:ResolveCase",
        "supportplans:GetSupportPlan",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:GetSupportPlanUpdateStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ActivateAdvancedProvisioningAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:CreateBuilderIdOwnedAccount",
        "organizations:DescribeCreateAccountStatus",
        "organizations:ListAccounts",
        "sso:ListInstances",
        "identitystore:GetUserId",
        "sso-directory:ListProvisioningTenants",
        "account-access:ListApplications",
        "account-access:CreateApplication",
        "account-access:CreateEntitlement",
        "signin:DeleteConsoleAuthorizationConfiguration",
        "signin:DeleteResourcePermissionStatement",
        "signin:ListResourcePermissionStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "ActivateAdvancedDelegatedAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com",
          "organizations:ServicePrincipal" : [
            "sso.amazonaws.com",
            "account-access.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ActivateAdvancedManagedRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:ListAttachedRolePolicies",
        "iam:DetachRolePolicy",
        "iam:ListRolePolicies",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/managed/*",
        "arn:aws:iam::*:role/ManagedAccountAdmin",
        "arn:aws:iam::*:role/AccountFullAccessRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ActivateAdvancedMemberAccountAssume",
```

```
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/managed/
AWSManagedAdvancedFeaturesActivationRole",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ActivateAdvancedBudgetsAccess",
      "Effect" : "Allow",
      "Action" : "budgets:ModifyBudget",
      "Resource" : "arn:aws:budgets::*:budget/sla-*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ActivateAdvancedSCPCleanupAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DeletePolicy",
        "organizations:DetachPolicy",
        "organizations:AttachPolicy",
        "organizations:CreatePolicy",
        "organizations:ListPolicies",
        "organizations:ListRoots"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceAccessForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com",
            "compute-optimizer.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForComputeOptimizerAutomation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/aco-automation.amazonaws.com/
AWSServiceRoleForComputeOptimizerAutomation",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "aco-automation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForComputeOptimizer",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/compute-
optimizer.amazonaws.com/AWSServiceRoleForComputeOptimizer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "compute-optimizer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cost-optimization-
hub.bcm.amazonaws.com/AWSServiceRoleForCostOptimizationHub",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cost-optimization-hub.bcm.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "GetAndUpdateEnrollmentStatusForACOCOH",
      "Effect" : "Allow",
      "Action" : [
        "aco-automation:GetEnrollmentConfiguration",
        "aco-automation:UpdateEnrollmentConfiguration",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:UpdateEnrollmentStatus",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:UpdateEnrollmentStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSManagedSettingsReadOnlyAccess

Descrição: Concede aos membros da equipe acesso somente para leitura às AWS Configurações, incluindo informações do espaço de trabalho e do proprietário, associação à equipe, plano e resumo dos gastos. Ele não concede permissões para modificar a configuração do espaço de trabalho ou gerenciar cobranças e pagamentos.

`AWSManagedSettingsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSManagedSettingsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 22 de julho de 2026, 01:12 UTC
- Horário editado: 21 de agosto de 2026, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagedSettingsReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccountReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetContactInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IdentityStoreReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroups",
        "identitystore:ListUsers"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "OrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeInstance"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSODirectoryReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSManagedSignUpAdminAccess

Descrição: Concede AWS permissão para concluir a inscrição em contas AWS gerenciadas.

`AWSManagedSignUpAdminAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSManagedSignUpAdminAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 20 de julho de 2026, 19:27 UTC
- Horário editado: 20 de julho de 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSManagedSignUpAdminAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PaymentWidgetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "payments:CreatePaymentInstrument",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "payments:ListTagsForResource",
        "payments:MakePayment",
```

```
        "payments:TagResource",
        "payments:UntagResource",
        "payments:UpdatePaymentInstrument",
        "payments:UpdatePaymentPreferences"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BillingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "billing:GetSellerOfRecord"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccountPermissions",
      "Effect" : "Allow",
      "Action" : [
        "account:GetContactInformation"
      ],
      "Resource" : "arn:aws:account::*:account"
    },
    {
      "Sid" : "InvoicingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "invoicing:GetInvoicePDF"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TaxWidgetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tax:BatchPutTaxRegistration",
        "tax:DeleteTaxRegistration",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "tax:PutTaxRegistration"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CustomerVerificationWidgetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "customer-verification:CreateCustomerVerificationDetails",
        "customer-verification:CreateUploadUrls",
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "customer-verification:UpdateCustomerVerificationDetails"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSManagementConsoleAdministratorAccess

Descrição: Fornece acesso total para configurar e personalizar o Console de gerenciamento da AWS

`AWSManagementConsoleAdministratorAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSManagementConsoleAdministratorAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de trabalho
- Horário de criação: 14 de agosto de 2025, 21:19 UTC
- Horário editado: 23 de março de 2026, 16:42 UTC

- ARN: `arn:aws:iam::aws:policy/job-function/AWSManagementConsoleAdministratorAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "uxc:GetAccountColor",
        "uxc:PutAccountColor",
        "uxc:DeleteAccountColor",
        "uxc:GetAccountCustomizations",
        "uxc:UpdateAccountCustomizations",
        "uxc:ListServices",
        "ec2:DescribeRegions",
        "notifications:GetFeatureOptInStatus",
        "notifications:AssociateChannel",
        "notifications:AssociateManagedNotificationAccountContact",
        "notifications:AssociateManagedNotificationAdditionalChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteEventRule",
        "notifications:DeleteNotificationConfiguration",
        "notifications:DeregisterNotificationHub",
        "notifications:DisableNotificationsAccessForOrganization",
        "notifications:DisassociateChannel",
        "notifications:DisassociateManagedNotificationAccountContact",
        "notifications:DisassociateManagedNotificationAdditionalChannel",
        "notifications:EnableNotificationsAccessForOrganization",
        "notifications:GetEventRule",
        "notifications:GetManagedNotificationChildEvent",
```

```
        "notifications:GetManagedNotificationConfiguration",
        "notifications:GetManagedNotificationEvent",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:GetNotificationsAccessForOrganization",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListManagedNotificationChildEvents",
        "notifications:ListManagedNotificationConfigurations",
        "notifications:ListManagedNotificationEvents",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:ListTagsForResource",
        "notifications:RegisterNotificationHub",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "cloudshell:CreateEnvironment",
        "cloudshell:CreateSession",
        "cloudshell:GetEnvironmentStatus",
        "cloudshell:DeleteEnvironment",
        "cloudshell:GetFileDownloadUrls",
        "cloudshell:GetFileUploadUrls",
        "cloudshell:DescribeEnvironments",
        "cloudshell:PutCredentials",
        "cloudshell:StartEnvironment",
        "cloudshell:StopEnvironment",
        "cloudshell:ApproveCommand",
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:DeleteIndex",
        "resource-explorer-2:DeleteView",
        "resource-explorer-2:DisassociateDefaultView",
        "resource-explorer-2:GetAccountLevelServiceConfiguration",
```

```
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetManagedView",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListIndexesForMembers",
        "resource-explorer-2:ListManagedViews",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:UpdateView",
        "action-recommendations:ListRecommendedActions",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSManagementConsoleBasicUserAccess

Descrição: Concede acesso a Console de gerenciamento da AWS recursos essenciais e capacidades de experiência do usuário (UX) para usuários não administrativos.

`AWSManagementConsoleBasicUserAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSManagementConsoleBasicUserAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 14 de agosto de 2025, 20:34 UTC
- Horário editado: 17 de março de 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagementConsoleBasicUserAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "uxc:GetAccountColor",
        "uxc:GetAccountCustomizations",
        "uxc:ListServices",
        "ec2:DescribeRegions",
        "notifications:GetFeatureOptInStatus",
        "notifications:ListManagedNotificationEvents",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:GetManagedNotificationChildEvent",
        "notifications:GetManagedNotificationEvent",
```

```
        "notifications:GetNotificationEvent",
        "notifications:ListManagedNotificationChildEvents",
        "cloudshell:CreateEnvironment",
        "cloudshell:CreateSession",
        "cloudshell:GetEnvironmentStatus",
        "cloudshell:StartEnvironment",
        "cloudshell:DeleteEnvironment",
        "cloudshell:PutCredentials",
        "cloudshell:StopEnvironment",
        "cloudshell:ApproveCommand",
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search",
        "action-recommendations:ListRecommendedActions",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplaceAmiIngestion

Descrição: Permite AWS Marketplace copiar suas imagens de máquina da Amazon (AMIs) para listá-las no AWS Marketplace

`AWSMarketplaceAmiIngestion` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMarketplaceAmiIngestion` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de setembro de 2020, 20:55 UTC
- Hora da edição: 25 de setembro de 2020, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:ec2:us-east-1::snapshot/snap-*"
    },
    {
      "Action" : [
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshotAttribute",
        "ec2:ModifyImageAttribute"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplaceDeploymentServiceRolePolicy

Descrição: permite AWS Marketplace criar e gerenciar parâmetros de implantação do vendedor para os produtos que você assina AWS Marketplace.

`AWSMarketplaceDeploymentServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 15 de novembro de 2023, 23:34 UTC
- Hora da edição: 15 de novembro de 2023, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageMarketplaceDeploymentSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:RemoveRegionsFromReplication"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:marketplace-deployment*!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TagMarketplaceDeploymentSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
```

```
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:marketplace-deployment!*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/expirationDate" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "expirationDate"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplaceDiscoveryFullAccess

Descrição: fornece acesso total à API AWS Marketplace Discovery para pesquisar e recuperar informações sobre produtos e preços.

`AWSMarketplaceDiscoveryFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMarketplaceDiscoveryFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 07 de maio de 2026, 17:12 UTC

- Horário editado: 07 de maio de 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceDiscoveryFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetListing",
        "aws-marketplace:GetProduct",
        "aws-marketplace:GetOffer",
        "aws-marketplace:GetOfferTerms",
        "aws-marketplace:GetOfferSet",
        "aws-marketplace:ListPurchaseOptions",
        "aws-marketplace:ListFulfillmentOptions",
        "aws-marketplace:SearchListings",
        "aws-marketplace:SearchFacets"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/product/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/listing/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offer/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offerSet/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/purchaseOption/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplaceFullAccess

Descrição: Fornece a capacidade de assinar e cancelar a assinatura de AWS Marketplace software, permite que os usuários gerenciem instâncias de software do Marketplace a partir da página “Seu software” do Marketplace e fornece acesso administrativo ao EC2.

`AWSMarketplaceFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMarketplaceFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de fevereiro de 2015, 17:21 UTC
- Horário editado: 11 de setembro de 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceFullAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeAddresses",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "license-manager:ListReceivedLicenses",
        "payments:ListPaymentProgramStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:CreateImage",
        "ec2:DescribeInstanceStatus",
        "ssm:GetAutomationExecution",
```

```
        "ssm:ListDocuments",
        "ssm:DescribeDocument",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:CreateTopic",
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:ListRoles",
        "iam:ListInstanceProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "signin:CreateOAuth2Token",
      "Resource" : "arn:aws:signin:*:*:service-principal/marketplace-
mcp.amazonaws.com",
      "Condition" : {
        "StringEquals" : {
          "signin:OAuthGrantType" : "client_credentials"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplaceGetEntitlements

Descrição: Fornece acesso de leitura aos AWS Marketplace direitos

`AWSMarketplaceGetEntitlements` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMarketplaceGetEntitlements` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de março de 2017, 19:37 UTC
- Hora da edição: 5 de abril de 2024, 1:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceGetEntitlements",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetEntitlements"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplaceImageBuildFullAccess

Descrição: Fornece acesso total ao recurso AWS Marketplace Private Image Build. Além de criar imagens privadas, ele também fornece permissões para adicionar tags às imagens, iniciar e encerrar instâncias ec2.

`AWSMarketplaceImageBuildFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMarketplaceImageBuildFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 31 de julho de 2018, 23:29 UTC
- Hora da edição: 04 de março de 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListBuilds",
        "aws-marketplace:StartBuild",
        "aws-marketplace:DescribeBuilds"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "ec2:ResourceTag/marketplace-image-build:build-id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*Automation*",
        "arn:aws:iam::*:role/*Instance*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:DescribeDocument",
        "ec2:DeregisterImage",
        "ec2:CopyImage",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DeleteSnapshot",
        "ec2:CreateImage",
        "ec2:RunInstances",
        "ec2:DescribeInstanceStatus",
        "sns:GetTopicAttributes",
        "iam:GetRole",
        "iam:GetInstanceProfile"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*image-build*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*image-build*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
        "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
        "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
        "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
        "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
        "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
        "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
        "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
            "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
            "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
            "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
            "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
            "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
            "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
            "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/marketplace-image-build:build-id" : "*"
        },
        "StringNotEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplaceLicenseManagementServiceRolePolicy

Descrição: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo AWS Marketplace para o gerenciamento de licenças.

`AWSMarketplaceLicenseManagementServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 3 de dezembro de 2020, 8:33 UTC
- Hora da edição: 3 de dezembro de 2020, 8:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowLicenseManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "license-manager:ListReceivedGrants",
        "license-manager:ListDistributedGrants",
        "license-manager:GetGrant",
        "license-manager:CreateGrant",
        "license-manager:CreateGrantVersion",
        "license-manager:DeleteGrant",
        "license-manager:AcceptGrant"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplaceManageSubscriptions

Descrição: Fornece a capacidade de assinar e cancelar a AWS Marketplace assinatura do software

`AWSMarketplaceManageSubscriptions` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMarketplaceManageSubscriptions` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 07 de maio de 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetListing",
        "aws-marketplace:GetProduct",
        "aws-marketplace:GetOffer",
        "aws-marketplace:GetOfferTerms",
        "aws-marketplace:GetOfferSet",
        "aws-marketplace:ListPurchaseOptions",
        "aws-marketplace:ListFulfillmentOptions",
        "aws-marketplace:SearchFacets",
        "aws-marketplace:SearchListings"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/product/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/listing/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offer/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offerSet/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/purchaseOption/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:UpdatePurchaseOrders",
        "aws-marketplace:ListAgreementCharges",
        "aws-marketplace:GetAgreementPaymentRequest",
        "aws-marketplace:ListAgreementPaymentRequests",
        "aws-marketplace:AcceptAgreementPaymentRequest",
        "aws-marketplace:RejectAgreementPaymentRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        },
        "Null" : {
```

```
          "aws-marketplace:AgreementType" : "false"
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceChangeSetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
    },
    {
      "Sid" : "AWSMarketplaceTokenManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/AgentTokenContainer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
            "CreateAgentTokenContainer",
            "RequestExpressPrivateOffer",
            "ExpireToken"
          ]
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceEntityReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceAgreementCancellationRequestAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListAgreementCancellationRequests",
        "aws-marketplace:GetAgreementCancellationRequest",
        "aws-marketplace:AcceptAgreementCancellationRequest",
        "aws-marketplace:CancelAgreement",
        "aws-marketplace:RejectAgreementCancellationRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        },
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Acceptor"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplaceMeteringFullAccess

Descrição: Fornece acesso total à AWS Marketplace medição.

`AWSMarketplaceMeteringFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMarketplaceMeteringFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de março de 2016, 22:39 UTC
- Hora da edição: 17 de março de 2016, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:MeterUsage"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplaceMeteringRegisterUsage

Descrição: Fornece permissões para registrar um recurso e rastrear o uso por meio do AWS Marketplace Metering Service.

`AWSMarketplaceMeteringRegisterUsage` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMarketplaceMeteringRegisterUsage` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 21 de novembro de 2019, 1:17 UTC
- Hora da edição: 21 de novembro de 2019, 1:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:RegisterUsage"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplaceProcurementSystemAdminFullAccess

Descrição: Fornece acesso total a todas as ações administrativas para uma integração de AWS Marketplace compras eletrônicas.

`AWSMarketplaceProcurementSystemAdminFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMarketplaceProcurementSystemAdminFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de junho de 2019, 13:07 UTC
- Horário editado: 21 de abril de 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*",
        "invoicing:CreateProcurementPortalPreference",
        "invoicing:GetProcurementPortalPreference",
        "invoicing:ListProcurementPortalPreferences"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplacePurchaseOrdersServiceRolePolicy

Descrição: Permite o acesso aos AWS Marketplace serviços de gerenciamento de pedidos de compra.

`AWSMarketplacePurchaseOrdersServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 27 de outubro de 2021, 15:12 UTC
- Hora da edição: 27 de outubro de 2021, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplaceRead-only

Descrição: Fornece a capacidade de revisar AWS Marketplace assinaturas

`AWSMarketplaceRead-only` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMarketplaceRead-only` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 07 de maio de 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceRead-only`

Versão da política

Versão da política: v13 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:ListAgreementCharges",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListInstanceProfiles",
        "sns:GetTopicAttributes",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests",
        "aws-marketplace:GetAgreementPaymentRequest",
        "aws-marketplace:ListAgreementPaymentRequests"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "aws-marketplace:GetListing",
        "aws-marketplace:GetProduct",
        "aws-marketplace:GetOffer",
        "aws-marketplace:GetOfferTerms",
        "aws-marketplace:GetOfferSet",
        "aws-marketplace:ListPurchaseOptions",
        "aws-marketplace:ListFulfillmentOptions",
        "aws-marketplace:SearchFacets",
        "aws-marketplace:SearchListings"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/product/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/listing/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offer/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/offerSet/*",
        "arn:aws:aws-marketplace:::catalog/AWSMarketplace*/purchaseOption/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListAgreementCancellationRequests",
        "aws-marketplace:GetAgreementCancellationRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplaceResaleAuthorizationServiceRolePolicy

Descrição: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pela AWS Marketplace para autorização de revenda.

`AWSMarketplaceResaleAuthorizationServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 5 de março de 2024, 18:47 UTC
- Horário editado: 01 de agosto de 2025, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMCreate",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ram:CreateResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ram:RequestedResourceType" : "aws-marketplace:Entity"
        },
        "ArnLike" : {
          "ram:ResourceArn" : "arn:aws:aws-marketplace:*:*:*/ResaleAuthorization/*"
        },
        "Null" : {
          "ram:Principal" : "true"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMAssociate",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "Null" : {
          "ram:Principal" : "false"
        },
        "StringEquals" : {
          "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMAcceptDelete",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:DeleteResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMGet",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ]
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplace",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:*/ResaleAuthorization/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplaceDescribe",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:*/ResaleAuthorization/*"
    }
  ]
```

```
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplaceSellerFullAccess

Descrição: fornece acesso total a todas as operações do vendedor no AWS Marketplace e em outros AWS serviços, como gerenciamento de AMI.

`AWSMarketplaceSellerFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMarketplaceSellerFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 02 de julho de 2019, 20:40 UTC
- Horário editado: 12 de agosto de 2026, 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess`

Versão da política

Versão da política: v33 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "MarketplaceManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace-management:uploadFiles",
        "aws-marketplace-management:viewReports",
        "aws-marketplace-management:viewSupport",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:GetSellerDashboard",
        "aws-marketplace:ListAssessments",
        "aws-marketplace:DescribeAssessment",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AgreementAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "AssetScanning",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VendorInsights",
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*",
        "arn:aws:aws-marketplace:*:*:catalog/AWSMarketplace*/*",
```

```
        "arn:aws:aws-marketplace:*:*:verification-type/*/verification-evidence/*",
        "arn:aws:aws-marketplace:*:*:tax-compliance-profile/*",
        "arn:aws:aws-marketplace:*:*:tax-compliance-profile-change-task/*"
      ]
    },
    {
      "Sid" : "SellerSettings",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace-management:GetSellerVerificationDetails",
        "aws-marketplace-management:PutSellerVerificationDetails",
        "aws-marketplace-management:GetBankAccountVerificationDetails",
        "aws-marketplace-management:PutBankAccountVerificationDetails",
        "aws-marketplace-management:GetSecondaryUserVerificationDetails",
        "aws-marketplace-management:PutSecondaryUserVerificationDetails",
        "aws-marketplace-management:GetAdditionalSellerNotificationRecipients",
        "aws-marketplace-management:PutAdditionalSellerNotificationRecipients",
        "payments:GetPaymentInstrument",
        "payments:CreatePaymentInstrument",
        "payments:DeletePaymentInstrument",
        "tax:GetTaxInterview",
        "tax:PutTaxInterview",
        "tax:GetTaxInfoReportingDocument",
        "tax:ListSupplementalTaxRegistrations",
        "tax:PutSupplementalTaxRegistration",
        "tax:DeleteSupplementalTaxRegistration",
        "tax:GetTaxRegistration",
        "tax:PutTaxRegistration",
        "tax:ListTaxRegistrations",
        "aws-marketplace:ListPayables",
        "aws-marketplace:ListInvoiceSubmissionTasks",
        "invoicing:ListInvoiceSummaries",
        "invoicing:GetInvoicePDF",
        "aws-marketplace:ListIssuedTaxInvoices"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceSellerVerificationEvidenceManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreateVerificationEvidence",
        "aws-marketplace:UpdateVerificationEvidence",
        "aws-marketplace:GetVerificationEvidence"
```

```
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:verification-type/*/verification-
evidence/*"
    },
    {
      "Sid" : "MarketplaceSellerVerificationManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListVerificationEvidence",
        "aws-marketplace:StartVerification",
        "aws-marketplace:GetVerification",
        "aws-marketplace:ListVerifications"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "InvoiceSubmissionManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartInvoiceSubmissionTask",
        "aws-marketplace:GetInvoiceSubmissionTask"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:catalog/AWSMarketplace*/invoice-
submission-task/*"
    },
    {
      "Sid" : "MarketplaceEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-files/
${aws:PrincipalAccount}/*"
      ]
    },
    {
      "Sid" : "Support",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ResourcePolicyManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*",
        "arn:aws:aws-marketplace:*:*:catalog/AWSMarketplace*/*"
      ]
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "resale-authorization.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AgreementPaymentRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SendAgreementPaymentRequest",
        "aws-marketplace:GetAgreementPaymentRequest",
        "aws-marketplace:ListAgreementPaymentRequests",
        "aws-marketplace:CancelAgreementPaymentRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VerificationAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:StartVerification",
        "partnercentral:GetVerification"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SellerSettingsGetIssuedTaxInvoice",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetIssuedTaxInvoice"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:catalog/AWSMarketplace*/issued-tax-
invoice/*"
    },
    {
      "Sid" : "AWSMarketplaceAgreementsCancellationAndAdjustmentAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListAgreementInvoiceLineItems",
        "aws-marketplace:ListBillingAdjustmentRequests",
        "aws-marketplace:GetBillingAdjustmentRequest",
        "aws-marketplace:BatchCreateBillingAdjustmentRequest",
        "aws-marketplace:ListAgreementCancellationRequests",
        "aws-marketplace:GetAgreementCancellationRequest",
        "aws-marketplace:SendAgreementCancellationRequest",
        "aws-marketplace:CancelAgreementCancellationRequest"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "TaxComplianceProfileChangeTaskManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartTaxComplianceProfileChangeTask"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:tax-compliance-profile-change-task/*"
    },
    {
      "Sid" : "TaxComplianceProfileRead",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetTaxComplianceProfile"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:tax-compliance-profile/*"
    },
    {
      "Sid" : "TaxComplianceProfileList",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListTaxComplianceProfileChangeTasks",
        "aws-marketplace:ListTaxComplianceProfiles"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplaceSellerOfferManagement

Descrição: fornece aos vendedores acesso às atividades de gerenciamento de ofertas e acordos.

`AWSMarketplaceSellerOfferManagement` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMarketplaceSellerOfferManagement` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 19 de novembro de 2024, 00:41 UTC
- Horário editado: 31 de março de 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerOfferManagement`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceChangeSetReadAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceOfferManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Offer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceCreateOfferOnProduct",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : "CreateOfferOnProduct"
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceListEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceEntitiesReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
```

```
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Offer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ContainerProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProfessionalServicesProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/SaaSProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/AmiProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAgreementsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceAgreementsCancellationAndAdjustmentReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListAgreementInvoiceLineItems",
        "aws-marketplace:ListBillingAdjustmentRequests",
        "aws-marketplace:GetBillingAdjustmentRequest",
        "aws-marketplace:ListAgreementCancellationRequests",
        "aws-marketplace:GetAgreementCancellationRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
```

```
          ]
        },
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplaceSellerProductsFullAccess

Descrição: Fornece aos vendedores acesso total à página AWS Marketplace de produtos de gerenciamento e a outros AWS serviços, como gerenciamento de AMI.

`AWSMarketplaceSellerProductsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMarketplaceSellerProductsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 02 de julho de 2019, 21:06 UTC
- Horário editado: 19 de fevereiro de 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess`

Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MarketplaceListAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:ListEntities",
        "aws-marketplace:ListAssessments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "MarketplaceAssessmentAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeAssessment"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "EC2ResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetIAMRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VendorInsightsAccess",
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "ResourceSharingAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "MarketplaceEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-files/
${aws:PrincipalAccount}/*"
      ]
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" :
 "TechnicalStaff"
        }
      }
```

```
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMarketplaceSellerProductsReadOnly

Descrição: Forneça aos vendedores acesso somente para leitura à página AWS Marketplace de produtos de gerenciamento.

`AWSMarketplaceSellerProductsReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMarketplaceSellerProductsReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 02 de julho de 2019, 21:40 UTC

- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListAssessments",
        "aws-marketplace:DescribeAssessment",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy"
      ],
```

```
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMcpServiceActionsFullAccess

Descrição: Fornece acesso total a todas as ações do serviço MCP. Essa política não concede acesso às ações tomadas pelo MCP, somente às ações do MCP em si.

`AWSMcpServiceActionsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMcpServiceActionsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 21 de novembro de 2025, 22:49 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMcpServiceActionsFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllMCPServiceActions",
      "Effect" : "Allow",
      "Action" : "*",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMCPSignInOAuthAccessPolicy

Descrição: Fornece acesso para autenticação no servidor AWS MCP usando OAuth AWS Sign-In

`AWSMCPSignInOAuthAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMCPSignInOAuthAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Tempo de criação: 09 de julho de 2026, 06:57 UTC
- Horário editado: 09 de julho de 2026, 06:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMCPSignInOAuthAccessPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOAuthForAWSMCP",
      "Effect" : "Allow",
      "Action" : [
        "signin:AuthorizeOAuth2Access",
        "signin:CreateOAuth2Token"
      ],
      "Resource" : "arn:aws:signin:*:*:service-principal/aws-mcp.amazonaws.com"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMediaConnectServicePolicy

Descrição: A política padrão que permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo MediaConnect.

`AWSMediaConnectServicePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 03 de abril de 2023, 22:11 UTC
- Horário editado: 29 de outubro de 2025, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:DeleteService",
```

```
        "ecs:CreateService",
        "ecs:DescribeServices",
        "ecs:PutAttributes",
        "ecs:DeleteAttributes",
        "ecs:RunTask",
        "ecs:ListTasks",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:UpdateContainerInstancesState"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateCluster",
        "ecs:UpdateClusterSettings",
        "ecs:ListAttributes",
        "ecs:DescribeClusters",
        "ecs:DeregisterContainerInstance",
        "ecs:ListContainerInstances"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
```

```
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/created-for-service" : "MediaConnect"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMediaLiveAnywhereServiceRolePolicy

Descrição: Permite que o MediaLive Anywhere crie e gerencie AWS recursos em seu nome.

`AWSMediaLiveAnywhereServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 14 de abril de 2025, 22:07 UTC
- Horário editado: 14 de abril de 2025, 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaLiveAnywhereServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PutMediaLiveMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/MediaLive"
        }
      }
    },
    {
      "Sid" : "RegisterAnywhereAgentTaskDefinition",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/MediaLiveAnywhereAgent*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/created_by" : "MediaLiveAnywhere"
        }
      }
    },
    {
      "Sid" : "ECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : "RegisterTaskDefinition",
          "aws:RequestTag/created_by" : "MediaLiveAnywhere"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "created_by"
        }
      }
    },
    {
      "Sid" : "UpdateAnywhereAgentService",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ecs:Cluster" : "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*",
          "ecs:Task-Definition" : "arn:aws:ecs:*:*:task-definition/
MediaLiveAnywhereAgent*"
        }
      }
    },
    {
```

```
      "Sid" : "ECSListTaskDefinitions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTaskDefinitions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeregisterAnywhereAgentTaskDefinitionOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeregisterTaskDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeleteAnywhereAgentTaskDefinitionsOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteTaskDefinitions"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/MediaLiveAnywhereAgent*"
      ]
    },
    {
      "Sid" : "DeleteAnywhereAgentServiceOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteService"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:service/MediaLiveAnywhere*/MediaLiveAnywhereAgent*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ecs:Cluster" : "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*"
        }
      }
    },
```

```
    {
      "Sid" : "DeregisterContainerInstanceOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListContainerInstances",
        "ecs:DeregisterContainerInstance"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMediaTailorServiceRolePolicy

Descrição: Habilitar o acesso aos AWS recursos usados ou gerenciados pelo MediaTailor

`AWSMediaTailorServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 17 de setembro de 2021, 22:27 UTC
- Hora da edição: 17 de setembro de 2021, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMigrationHubDiscoveryAccess

Descrição: A política AWSMigrationHubService permite ligar AWSApplicationDiscoveryService em nome do cliente.

`AWSMigrationHubDiscoveryAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMigrationHubDiscoveryAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 14 de agosto de 2017, 13:30 UTC
- Hora da edição: 06 de agosto de 2020, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "dms:AddTagsToResource",
      "Resource" : [
        "arn:aws:dms:*:*:endpoint:*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMigrationHubDMSAccess

Descrição: política que permite que o Database Migration Service assuma um perfil na conta do cliente para chamar o Migration Hub

`AWSMigrationHubDMSAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMigrationHubDMSAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 14 de agosto de 2017, 14:00 UTC
- Hora da edição: 07 de outubro de 2019, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:CreateProgressUpdateStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS"
    },
```

```
    {
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:AssociateDiscoveredResource",
        "mgh:DisassociateDiscoveredResource",
        "mgh:ListDiscoveredResources"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/*"
    },
    {
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:GetHomeRegion"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMigrationHubFullAccess

Descrição: política gerenciada para fornecer ao cliente acesso ao Migration Hub Service

`AWSMigrationHubFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMigrationHubFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de agosto de 2017, 14:02 UTC
- Hora da edição: 19 de junho de 2019, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:*",
        "discovery:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "migrationhub.amazonaws.com",
            "dmsintegration.migrationhub.amazonaws.com",
            "smsintegration.migrationhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMigrationHubOrchestratorConsoleFullAccess

Descrição: Fornece acesso limitado ao AWS Migration Hub, ao AWS Application Discovery Service, ao Amazon Simple Storage Service e ao AWS Secrets Manager. Essa política também concede acesso total ao serviço AWS Migration Hub Orchestrator.

`AWSMigrationHubOrchestratorConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMigrationHubOrchestratorConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 20 de abril de 2022, 2:26 UTC
- Hora da edição: 5 de dezembro de 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHO",
```

```
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "S3MHO",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::migrationhub-orchestrator-*/*"
      ]
    },
    {
      "Sid" : "ListSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Configuration",
      "Effect" : "Allow",
      "Action" : [
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations",
```

```
        "discovery:GetDiscoverySummary"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetHomeRegion",
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMListProfileRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListClusters"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Account",
      "Effect" : "Allow",
      "Action" : [
        "account:ListRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "migrationhub-orchestrator.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/migrationhub-
orchestrator.amazonaws.com/AWSServiceRoleForMigrationHubOrchestrator*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMigrationHubOrchestratorInstanceRolePolicy

Descrição: esta política precisa ser anexada à instância migrada para SAP e MGN para que nosso serviço orquestre instâncias ao baixar scripts do S3 e buscar valores secretos dentro da instância do EC2.

`AWSMigrationHubOrchestratorInstanceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMigrationHubOrchestratorInstanceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 20 de abril de 2022, 2:43 UTC
- Hora da edição: 20 de abril de 2022, 2:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
```

```
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::aws-migrationhub-orchestrator-*/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMigrationHubOrchestratorPlugin

Descrição: Fornece acesso limitado às ações relacionadas ao Amazon Simple Storage Service, AWS Secrets Manager e Plugin para o AWS Migration Hub Orchestrator.

`AWSMigrationHubOrchestratorPlugin` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMigrationHubOrchestratorPlugin` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 20 de abril de 2022, 2:25 UTC
- Hora da edição: 20 de abril de 2022, 2:25 UTC

- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-orchestrator-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : [
        "arn:aws:execute-api:*:*:*/prod/*/put-log-data",
        "arn:aws:execute-api:*:*:*/prod/*/put-metric-data"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:RegisterPlugin",
        "migrationhub-orchestrator:GetMessage",
        "migrationhub-orchestrator:SendMessage"
      ],
      "Resource" : "arn:aws:migrationhub-orchestrator:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMigrationHubOrchestratorServiceRolePolicy

Descrição: fornece as permissões necessárias para que o Migration Hub Orchestrator migre e modernize seus workloads on-premises

`AWSMigrationHubOrchestratorServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 20 de abril de 2022, 2:24 UTC
- Hora da edição: 4 de março de 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationDiscoveryService",
      "Effect" : "Allow",
      "Action" : [
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LaunchWizard",
      "Effect" : "Allow",
      "Action" : [
        "launchwizard:ListProvisionedApps",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:ListDeployments",
        "launchwizard:GetDeployment"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "EC2instances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ec2MGNLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "mgn.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ec2LaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeLaunchTemplates"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "getHomeRegion",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMcommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
```

```
        "ssm:GetCommandInvocation",
        "ssm:CancelCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:s3:::aws-migrationhub-orchestrator-*",
        "arn:aws:s3:::migrationhub-orchestrator-*"
      ]
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "s3GetObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::migrationhub-orchestrator-*/*"
      ]
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:DeleteRule",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/MigrationHubOrchestratorManagedRule*"
    },
```

```
    {
      "Sid" : "MGN",
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetReplicationConfiguration",
        "mgn:GetLaunchConfiguration",
        "mgn:StartCutover",
        "mgn:FinalizeCutover",
        "mgn:StartTest",
        "mgn:UpdateReplicationConfiguration",
        "mgn:DescribeSourceServers",
        "mgn:MarkAsArchived",
        "mgn:ChangeServerLifeCycleState"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ec2DescribeImportImage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImportImageTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "s3ListBucket",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : "migrationhub-orchestrator-vmie-*"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

Descrição: Concede acesso total aos AWS Migration Hub Refactor Spaces e outros serviços AWS relacionados, exceto AWS Transit Gateway e grupos de segurança do EC2, que não são necessários ao usar ambientes sem uma ponte de rede. Essa política também exclui as permissões necessárias para o AWS Lambda e o AWS Resource Access Manager, pois elas podem ser reduzidas com base em tags.

`AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 03 de abril de 2023, 20:09 UTC
- Hora da edição: 11 de abril de 2024, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagsDelete",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationDelete",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ELBModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
```

```
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Sid" : "ELBListenerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBListenerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Sid" : "ELBTargetGroupModify",
      "Effect" : "Allow",
```

```
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Sid" : "ELBTargetGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayModify",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:UpdateRestApiPolicy"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "APIGatewayVpcLinksGet",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "OrganizationDescribe",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackTag",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*"
    },
    {
      "Sid" : "CreateRefactorSpacesSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "CreateELBSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

Descrição: Use na função de serviço IAM passada para o documento SSM Automation AWSRefactorSpaces-CreateResources para conceder as permissões necessárias para executar a automação. A política concede read/write acesso às tags do EC2 para acompanhar o progresso da automação. Quando a ponte de rede do ambiente do Refactor Spaces é ativada, a automação também adiciona o grupo de segurança do ambiente à instância do EC2 para permitir o tráfego de outros serviços do Refactor Spaces no ambiente. A política também concede acesso aos parâmetros SSM das ações pós-lançamento do Application Migration Service.

`AWSMigrationHubRefactorSpaces-SSMAutomationPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMigrationHubRefactorSpaces-SSMAutomationPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 10 de agosto de 2023, 15:08 UTC
- Hora da edição: 10 de agosto de 2023, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "refactor-spaces:ssm:environment-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMigrationHubRefactorSpacesFullAccess

Descrição: Concede acesso total aos recursos do console AWS MigrationHub Refactor Spaces, AWS MigrationHub Refactor Spaces e outros AWS serviços relacionados, exceto as permissões necessárias para o AWS Lambda e o AWS Resource Access Manager, pois eles podem ser definidos com base em tags.

`AWSMigrationHubRefactorSpacesFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMigrationHubRefactorSpacesFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2021, 7:12 UTC
- Hora da edição: 11 de abril de 2024, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RequestTagTransitGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "ResourceTagTransitGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2NetworkingModify",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTransitGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationDelete",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "ELBLoadBalancerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ELBModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Sid" : "ELBListenerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBListenerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Sid" : "ELBTargetGroupModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
```

```
      "Sid" : "ELBTargetGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayModify",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:UpdateRestApiPolicy"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayVpcLinksGet",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/vpclinks",
```

```
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "OrganizationDescribe",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackTag",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*"
    },
    {
      "Sid" : "CreateRefactorSpacesSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateELBSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMigrationHubRefactorSpacesServiceRolePolicy

Descrição: Fornece acesso aos AWS recursos gerenciados ou usados pelo AWS Migration Hub Refactor Spaces.

`AWSMigrationHubRefactorSpacesServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 29 de novembro de 2021, 6:50 UTC
- Hora da edição: 20 de julho de 2023, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:DeleteTags",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:PUT",
        "apigateway:POST",
        "apigateway:GET",
        "apigateway:PATCH",
        "apigateway:DELETE"
      ],
```

```
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : "arn:aws:apigateway:*::/vpclinks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMigrationHubSMSAccess

Descrição: política que permite que o Server Migration Service assuma um perfil na conta do cliente para chamar o Migration Hub

`AWSMigrationHubSMSAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMigrationHubSMSAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 14 de agosto de 2017, 13:57 UTC
- Hora da edição: 07 de outubro de 2019, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:CreateProgressUpdateStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS"
    },
    {
      "Action" : [
```

```
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:AssociateDiscoveredResource",
        "mgh:DisassociateDiscoveredResource",
        "mgh:ListDiscoveredResources"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/*"
    },
    {
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:GetHomeRegion"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMigrationHubStrategyCollector

Descrição: Concede permissões para permitir a comunicação com o serviço de recomendações estratégicas do AWS Migration Hub, read/write acesso aos buckets do S3 relacionados ao serviço, acesso ao Amazon API Gateway para fazer upload de registros e métricas AWS, acesso ao AWS Secrets Manager para buscar credenciais e quaisquer serviços relacionados.

`AWSMigrationHubStrategyCollector` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMigrationHubStrategyCollector` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 19 de outubro de 2021, 20:15 UTC
- Hora da edição: 1º de abril de 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHSRAllowS3Resources",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:ListBucket",
        "s3:GetBucketLocation"
```

```
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MHSRAllowS3ListBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MHSRAllowMetricsAndLogs",
      "Effect" : "Allow",
      "Action" : [
        "application-transformation:PutMetricData",
        "application-transformation:PutLogData",
        "application-transformation:StartPortingCompatibilityAssessment",
        "application-transformation:GetPortingCompatibilityAssessment",
        "application-transformation:StartPortingRecommendationAssessment",
        "application-transformation:GetPortingRecommendationAssessment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MHSRAllowExecuteAPI",
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : [
        "arn:aws:execute-api:*:*:*/prod/*/put-log-data",
        "arn:aws:execute-api:*:*:*/prod/*/put-metric-data"
```

```
      ]
    },
    {
      "Sid" : "MHSRAllowCollectorAPI",
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-strategy:RegisterCollector",
        "migrationhub-strategy:GetAntiPattern",
        "migrationhub-strategy:GetMessage",
        "migrationhub-strategy:SendMessage",
        "migrationhub-strategy:ListAntiPatterns",
        "migrationhub-strategy:ListJarArtifacts",
        "migrationhub-strategy:UpdateCollectorConfiguration",
        "migrationhub-strategy:PutLogData",
        "migrationhub-strategy:PutMetricData"
      ],
      "Resource" : "arn:aws:migrationhub-strategy:*:*:*"
    },
    {
      "Sid" : "MHSRAllowSecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-strategy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMigrationHubStrategyConsoleFullAccess

Descrição: Concede acesso total ao serviço de recomendações estratégicas do AWS Migration Hub e acesso aos AWS serviços relacionados por meio do Console de gerenciamento da AWS.

`AWSMigrationHubStrategyConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMigrationHubStrategyConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 19 de outubro de 2021, 20:13 UTC
- Hora da edição: 09 de novembro de 2022, 0:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-strategy:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:GetDiscoverySummary",
        "discovery:DescribeTags",
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "migrationhub-strategy.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/migrationhub-
strategy.amazonaws.com/AWSMigrationHubStrategyServiceRolePolicy*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMigrationHubStrategyServiceRolePolicy

Descrição: habilite o acesso aos AWS recursos usados ou gerenciados pelo serviço de recomendações estratégicas do AWS Migration Hub.

`AWSMigrationHubStrategyServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 19 de outubro de 2021, 20:02 UTC

- Hora da edição: 19 de outubro de 2021, 20:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "permissionsForAds",
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "permissionsForS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
```

```
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMobileHub_FullAccess

Descrição: Essa política pode ser anexada a qualquer usuário, função ou grupo, a fim de conceder aos usuários permissão para criar, excluir e modificar projetos (e seus AWS recursos associados) no AWS Mobile Hub. Isso também inclui permissões para gerar e baixar amostras de código-fonte do aplicativo móvel para cada projeto do Mobile Hub.

`AWSMobileHub_FullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMobileHub_FullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 05 de janeiro de 2016, 19:56 UTC
- Hora da edição: 19 de dezembro de 2019, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_FullAccess`

Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "cloudfront:GetDistribution",
        "devicefarm:CreateProject",
        "devicefarm:ListJobs",
        "devicefarm:ListRuns",
        "devicefarm:GetProject",
        "devicefarm:GetRun",
        "devicefarm:ListArtifacts",
        "devicefarm:ListProjects",
        "devicefarm:ScheduleRun",
        "dynamodb:DescribeTable",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "iam:ListSAMLProviders",
        "lambda:ListFunctions",
        "sns:ListTopics",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetBot",
        "lex:GetBots",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "mobilehub:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/aws-my-sample-app*.zip"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*-mobilehub-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*-mobilehub-*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMobileHub_ReadOnly

Descrição: Essa política pode ser anexada a qualquer usuário, função ou grupo, a fim de conceder aos usuários permissão para listar e visualizar projetos no AWS Mobile Hub. Isso também inclui permissões para gerar e baixar amostras de código-fonte do aplicativo móvel para cada projeto do Mobile Hub. Ele não permite que o usuário modifique nenhuma configuração para nenhum projeto do Mobile Hub.

`AWSMobileHub_ReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMobileHub_ReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 05 de janeiro de 2016, 19:55 UTC
- Hora da edição: 23 de julho de 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "iam:ListSAMLProviders",
        "lambda:ListFunctions",
        "sns:ListTopics",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetBot",
        "lex:GetBots",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "mobilehub:ExportProject",
```

```
        "mobilehub:GenerateProjectParameters",
        "mobilehub:GetProject",
        "mobilehub:SynchronizeProject",
        "mobilehub:GetProjectSnapshot",
        "mobilehub:ListProjectSnapshots",
        "mobilehub:ListAvailableConnectors",
        "mobilehub:ListAvailableFeatures",
        "mobilehub:ListAvailableRegions",
        "mobilehub:ListProjects",
        "mobilehub:ValidateProject",
        "mobilehub:VerifyServiceRole",
        "mobilehub:DescribeBundle",
        "mobilehub:ExportBundle",
        "mobilehub:ListBundles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/aws-my-sample-app*.zip"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSMSKReplicatorExecutionRole

Descrição: concede permissões ao Amazon MSK Replicator para replicar dados entre clusters do MSK.

`AWSMSKReplicatorExecutionRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSMSKReplicatorExecutionRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 6 de dezembro de 2023, 0:07 UTC
- Hora da edição: 25 de março de 2024, 21:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:Connect",
        "kafka-cluster:DescribeCluster",
        "kafka-cluster:AlterCluster",
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration",
```

```
        "kafka-cluster:WriteDataIdempotently"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "TopicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration",
        "kafka-cluster:AlterCluster"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:topic/*/*"
      ]
    },
    {
      "Sid" : "GroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:group/*/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSNATGatewayServiceRolePolicy

Descrição: fornece permissões para gerenciar recursos de VPC para a configuração e o gerenciamento de gateways NAT.

`AWSNATGatewayServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 14 de novembro de 2025, 17:19 UTC
- Horário editado: 14 de novembro de 2025, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNATGatewayServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSNetworkFirewallFullAccess

Descrição: Concede acesso total ao serviço AWS Network Firewall, incluindo permissões para criar, configurar, gerenciar e excluir recursos, políticas e grupos de regras do firewall. Além disso, inclui permissões para modificar endpoints de VPC, políticas de bucket do S3, configurações de CloudWatch registros e criar funções vinculadas a serviços para Network Firewall e serviços de entrega de registros

`AWSNetworkFirewallFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSNetworkFirewallFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 10 de junho de 2025, 21:52 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkFirewallFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewall",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListAnalysisReports",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListFlowOperations",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeFlowOperation",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:GetAnalysisReportResults",
        "network-firewall:ListFlowOperationResults",
        "network-firewall:TagResource",
        "network-firewall:UntagResource",
        "network-firewall:AssociateFirewallPolicy",
        "network-firewall:AssociateSubnets",
        "network-firewall:CreateFirewall",
        "network-firewall:CreateFirewallPolicy",
        "network-firewall:CreateRuleGroup",
        "network-firewall:CreateTLSInspectionConfiguration",
        "network-firewall:DeleteFirewall",
```

```
        "network-firewall:DeleteFirewallPolicy",
        "network-firewall:DeleteResourcePolicy",
        "network-firewall:DeleteRuleGroup",
        "network-firewall:DeleteTLSInspectionConfiguration",
        "network-firewall:DisassociateSubnets",
        "network-firewall:PutResourcePolicy",
        "network-firewall:StartAnalysisReport",
        "network-firewall:StartFlowCapture",
        "network-firewall:StartFlowFlush",
        "network-firewall:UpdateFirewallAnalysisSettings",
        "network-firewall:UpdateFirewallDeleteProtection",
        "network-firewall:UpdateFirewallDescription",
        "network-firewall:UpdateFirewallEncryptionConfiguration",
        "network-firewall:UpdateFirewallPolicy",
        "network-firewall:UpdateFirewallPolicyChangeProtection",
        "network-firewall:UpdateLoggingConfiguration",
        "network-firewall:UpdateRuleGroup",
        "network-firewall:UpdateSubnetChangeProtection",
        "network-firewall:UpdateTLSInspectionConfiguration"
      ],
      "Resource" : [
        "arn:aws:network-firewall:*:*:*"
      ]
    },
    {
      "Sid" : "NetworkFirewallEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallCreateVpcEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallDeleteVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallLogging",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallLoggingCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Sid" : "NetworkFirewallLoggingS3",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallLoggingFirehose",
      "Effect" : "Allow",
      "Action" : "firehose:TagDeliveryStream",
      "Resource" : "arn:aws:firehose:*:*:*"
    },
    {
      "Sid" : "NetworkFirewallSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/network-firewall.amazonaws.com/
AWSServiceRoleForNetworkFirewall"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "network-firewall.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallLogDeliverySLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSNetworkFirewallReadOnlyAccess

Descrição: fornece acesso somente para leitura aos recursos do AWS Network Firewall por meio da CLI e dos Console de gerenciamento da AWS SDKs. Essa política permite que os usuários visualizem e monitorem as configurações de firewall, as políticas, os grupos de regras e os recursos associados, mas sem a capacidade de fazer alterações.

`AWSNetworkFirewallReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSNetworkFirewallReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 10 de junho de 2025, 21:52 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkFirewallReadOnlyAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListAnalysisReports",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListFlowOperations",
        "network-firewall:ListProxies",
        "network-firewall:ListProxyConfigurations",
        "network-firewall:ListProxyRuleGroups",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:ListVpcEndpointAssociations",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallMetadata",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeFlowOperation",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeProxy",
        "network-firewall:DescribeProxyConfiguration",
        "network-firewall:DescribeProxyRule",
        "network-firewall:DescribeProxyRuleGroup",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:DescribeVpcEndpointAssociation",
        "network-firewall:GetAnalysisReportResults",
        "network-firewall:ListFlowOperationResults"
      ],
      "Resource" : "arn:aws:network-firewall:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries"
```

```
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSNetworkFirewallServiceRolePolicy

Descrição: Permite AWSNetworkFirewall criar e gerenciar os recursos necessários para seus firewalls.

`AWSNetworkFirewallServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 17 de novembro de 2020, 17:17 UTC
- Horário editado: 01 de junho de 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "acm:DescribeCertificate",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroupResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "resource-groups.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListContainerInstances",
        "ecs:ListTasks",
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*",
        "arn:aws:ecs:*:*:container-instance/*/*",
        "arn:aws:ecs:*:*:task/*/*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSNetworkManagerCloudWANServiceRolePolicy

Descrição: Permitir NetworkManager o acesso aos recursos associados à sua rede principal

`AWSNetworkManagerCloudWANServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 12 de julho de 2022, 12:17 UTC
- Hora da edição: 12 de julho de 2022, 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSNetworkManagerFullAccess

Descrição: Fornece acesso total à Amazon NetworkManager por meio do Console de gerenciamento da AWS.

`AWSNetworkManagerFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSNetworkManagerFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 03 de dezembro de 2019, 17:37 UTC
- Hora da edição: 03 de dezembro de 2019, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "networkmanager:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "networkmanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSNetworkManagerReadOnlyAccess

Descrição: Fornece acesso somente para leitura à Amazon NetworkManager por meio do Console de gerenciamento da AWS.

`AWSNetworkManagerReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSNetworkManagerReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 03 de dezembro de 2019, 17:35 UTC
- Hora da edição: 03 de dezembro de 2019, 17:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:Describe*",
        "networkmanager:Get*",
        "networkmanager:List*"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSNetworkManagerServiceRolePolicy

Descrição: Permitir NetworkManager acessar recursos associados às suas redes globais

`AWSNetworkManagerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 03 de dezembro de 2019, 14:03 UTC
- Hora da edição: 27 de julho de 2022, 19:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeLocations",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpcs",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeRegions",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:GetTransitGatewayPolicyTableEntries"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSObservabilityAdminLogsCentralizationServiceRolePolicy

Descrição: permissões de Service-linked função para centralização CloudWatch de registros

`AWSObservabilityAdminLogsCentralizationServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 15 de setembro de 2025, 14:34 UTC
- Horário editado: 15 de setembro de 2025, 14:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminLogsCentralizationServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "logs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/LogsManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:logs:arn" : "arn:aws:logs:*:*:log-group:*"
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSObservabilityAdminServiceRolePolicy

Descrição: Fornece acesso para gerenciar o AWS Config Configuration Recorder, gerenciar o AWS Config Configuration Aggregator, criar a função vinculada ao serviço de AWS configuração para a funcionalidade do Configuration Recorder, consumir dados de configuração do gravador e ler os dados da organização para obter recursos organizacionais. AWS

`AWSObservabilityAdminServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 27 de novembro de 2024, 19:36 UTC
- Horário editado: 14 de julho de 2026, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForObservabilityAdmin/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigurationAggregator",
        "config:DeleteConfigurationAggregator",
        "config:SelectAggregateResourceConfig"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
observabilityadmin.amazonaws.com/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "observabilityadmin.amazonaws.com",
            "config.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSObservabilityAdminTelemetryEnablementServiceRolePolicy

Descrição: Fornece acesso para gerenciar os recursos do gravador de AWS configuração e as configurações de telemetria em AWS recursos, incluindo registros e métricas.

`AWSObservabilityAdminTelemetryEnablementServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 01 de agosto de 2025, 18:04 UTC
- Horário editado: 23 de setembro de 2026, 22:27 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminTelemetryEnablementServiceRolePolicy`

Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TelemetryOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeFlowLogs",
        "ec2:DescribeVpcs",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "logs:ListLogGroups",
        "ec2:MonitorInstances",
        "logs:DescribeDeliverySources",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliveryDestinations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagOperationForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        },
        "StringEquals" : {
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : "CreateFlowLogs"
        }
      }
    },
    {
      "Sid" : "TagOperationForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForVPCLogs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFlowLogs"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "TelemetryOperationsForVPCFlowLogs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFlowLogs"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-flow-log/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        },
        "StringEquals" : {
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteFlowLogs",
        "logs:CreateDelivery",
        "logs:CreateLogGroup",
        "logs:PutResourcePolicy",
        "logs:PutRetentionPolicy",
        "logs:PutDeliveryDestination",
        "logs:PutDeliverySource",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSApiLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
```

```
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "Bool" : {
          "eks:loggingType/api" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "Bool" : {
          "eks:loggingType/audit" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSAuthenticatorLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "Bool" : {
          "eks:loggingType/authenticator" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSControllerManagerLogs",
```

```
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "Bool" : {
          "eks:loggingType/controllerManager" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSSchedulerLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "Bool" : {
          "eks:loggingType/scheduler" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForWafLoggingConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration"
      ],
      "Resource" : "arn:aws:wafv2:*:*:*/webacl/*",
      "Condition" : {
        "ArnLike" : {
          "wafv2:LogDestinationResource" : "arn:aws:logs:*:*:log-group:*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "wafv2:LogScope" : "CloudwatchTelemetryRuleManaged"
```

```
        }
      }
    },
    {
      "Sid" : "TelemetryReadForWafLoggingConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:ListLoggingConfigurations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForWafLogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:AllowVendedLogDeliveryForResource",
        "bedrock:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForSecurityHub",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:AllowVendedLogDeliveryForResource",
        "securityhub:DescribeHub",
        "securityhub:DescribeSecurityHubV2"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "TelemetryOperationsForCloudfront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForCloudTrailLogs",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:UpdateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/cloudwatch/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForManagedLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutResourcePolicy",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws/cloudtrail",
        "arn:aws:logs:*:*:log-group:aws/cloudtrail/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingListOperations",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverQueryLogConfigAssociations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingGetOperations",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingConfigCreation",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:CreateResolverQueryLogConfig",
        "route53resolver:TagResource"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:resolver-query-log-config/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingConfigAssociation",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:AssociateResolverQueryLogConfig"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForRoute53LogDeliverySLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:*:iam::*:role/aws-service-role/route53resolver.amazonaws.com/
AWSServiceRoleForRoute53Resolver",
      "Condition" : {
        "BoolIfExists" : {
          "aws:ViaAWSService" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:AWSServiceName" : [
            "route53resolver.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForRoute53LogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "IAMOperationsForConfigServiceLinkedRecorder",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "BoolIfExists" : {
          "aws:ViaAWSService" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:AWSServiceName" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManagementOperationsForServiceLinkedRecorder",
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:AssociateResourceTypes",
        "config:DisassociateResourceTypes"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForObservabilityAdmin_TelemetryEnablement/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReadOperationsForServiceLinkedRecorder",
```

```
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "config:ConfigurationRecorderServicePrincipal" : [
            "telemetry-enablement.observabilityadmin.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForKafka",
      "Effect" : "Allow",
      "Action" : [
        "kafka:UpdateMonitoring",
        "kafka:DescribeCluster"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForOTelEnrichmentSimba",
      "Effect" : "Allow",
      "Action" : [
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:StartTelemetryEnrichment",
        "observabilityadmin:StopTelemetryEnrichment"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "TelemetryOperationsForOTelEnrichmentResourceExplorer",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateManagedView",
        "resource-explorer-2:CreateStreamingAccessForService",
        "resource-explorer-2:DeleteStreamingAccessForService"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForOTelEnrichmentCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetOTelEnrichment",
        "cloudwatch:StartOTelEnrichment"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForOTelEnrichmentSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/*",
      "Condition" : {
        "Bool" : {
```

```
          "aws:ViaAWSService" : "true"
        },
        "StringEquals" : {
          "iam:AWSServiceName" : "resource-explorer-2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "TelemetryReadTagsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryKMSOperationsForAccount",
      "Effect" : "Allow",
      "Action" : [
        "kms:Describe*",
        "logs:AssociateKmsKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryKMSOperationsForOrganization",
      "Effect" : "Allow",
      "Action" : [
        "kms:Describe*",
        "logs:AssociateKmsKey"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:PrincipalOrgId" : "${aws:ResourceOrgId}"
        }
      }
    },
    {
      "Sid" : "InspectTemplate",
      "Effect" : "Allow",
      "Action" : "iam:GetRoleTemplateVersion",
      "Resource" : "arn:aws:iam::aws:role-template/telemetry-
enablement.observabilityadmin.amazonaws.com/
CloudWatchTelemetryRuleEKSAddonRoleTemplate:1"
    },
    {
      "Sid" : "AcquireRoleFromTemplate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
CloudWatchTelemetryRuleEKSAddonRole",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:RoleTemplateARN" : "arn:aws:iam::aws:role-
template/telemetry-enablement.observabilityadmin.amazonaws.com/
CloudWatchTelemetryRuleEKSAddonRoleTemplate:1"
        }
      }
    },
    {
      "Sid" : "AttachManagedPolicyFromTemplate",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Resource" : "arn:aws:iam::*:role/service-role/
CloudWatchTelemetryRuleEKSAddonRole",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
```

```
          "iam:RoleTemplateARN" : "arn:aws:iam::aws:role-
template/telemetry-enablement.observabilityadmin.amazonaws.com/
CloudWatchTelemetryRuleEKSAddonRoleTemplate:1"
        }
      }
    },
    {
      "Sid" : "ReadRole",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchTelemetryRuleEKSAddonRole",
        "arn:aws:iam::*:role/CloudWatchTelemetryRuleEKSAddonRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassRoleToPodIdentity",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
CloudWatchTelemetryRuleEKSAddonRole",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : "pods.eks.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InstallAddon",
      "Effect" : "Allow",
      "Action" : "eks:CreateAddon",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "FixAddon",
      "Effect" : "Allow",
      "Action" : "eks:UpdateAddon",
      "Resource" : "arn:aws:eks:*:*:addon/*/amazon-cloudwatch-observability/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreatePodIdentityAssociation",
      "Effect" : "Allow",
      "Action" : "eks:CreatePodIdentityAssociation",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FixPodIdentityAssociation",
      "Effect" : "Allow",
      "Action" : "eks:UpdatePodIdentityAssociation",
      "Resource" : "arn:aws:eks:*:*:podidentityassociation/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EvaluateAddon",
      "Effect" : "Allow",
      "Action" : "eks:DescribeAddon",
      "Resource" : "arn:aws:eks:*:*:addon/*/amazon-cloudwatch-observability/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "ListPodIdentityAssociations",
      "Effect" : "Allow",
      "Action" : "eks:ListPodIdentityAssociations",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EvaluatePodIdentityAssociation",
      "Effect" : "Allow",
      "Action" : "eks:DescribePodIdentityAssociation",
      "Resource" : "arn:aws:eks:*:*:podidentityassociation/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSOrganizationsFullAccess

Descrição: Fornece acesso total às AWS organizações.

`AWSOrganizationsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSOrganizationsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de novembro de 2018, 20:31 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsFullAccess`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsFullAccess",
      "Effect" : "Allow",
      "Action" : "organizations:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:PutAlternateContact",
        "account:DeleteAlternateContact",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:PutContactInformation",
        "account:ListRegions",
        "account:EnableRegion",
        "account:DisableRegion",
        "account:PutAccountName",
        "account:GetAccountInformation"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "organizations.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSOrganizationsReadOnlyAccess

Descrição: Fornece acesso somente para AWS leitura às organizações.

`AWSOrganizationsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSOrganizationsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de novembro de 2018, 20:32 UTC

- Hora da edição: 7 de junho de 2024, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsReadOnlyAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:ListRegions",
        "account:GetRegionOptStatus",
        "account:GetPrimaryEmail"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSOrganizationsServiceTrustPolicy

Descrição: Uma política para permitir que AWS as organizações compartilhem a confiança com outras aprovadas com Serviços da AWS o objetivo de simplificar a configuração do cliente.

`AWSOrganizationsServiceTrustPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 10 de outubro de 2017, 23:04 UTC
- Horário editado: 05 de março de 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDeletionOfServiceLinkedRoleForOrganizations",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/organizations.amazonaws.com/*"
      ]
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListRolesSLR",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSOutpostsAuthorizeServerPolicy

Descrição: esta política concede permissões que permitem que você instale um servidor Outpost em sua rede on-premises.

`AWSOutpostsAuthorizeServerPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSOutpostsAuthorizeServerPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 04 de janeiro de 2023, 19:23 UTC
- Hora da edição: 04 de janeiro de 2023, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:StartConnection",
        "outposts:GetConnection"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSOutpostsServiceRolePolicy

Descrição: Política de função vinculada ao serviço para permitir o acesso aos AWS recursos gerenciados pelo AWS Outposts

`AWSOutpostsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 09 de novembro de 2020, 22:55 UTC
- Horário editado: 17 de abril de 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "PrivateConnectivityServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateConnectivityCreateNetworkInterfacePolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*",
        "arn:*:ec2:*:*:subnet/*",
        "arn:*:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "PrivateConnectivityCreateNetworkInterfaceTaggingPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "outposts:private-connectivity-resourceId"
          ]
        }
      }
    },
    {
      "Sid" : "PrivateConnectivityCreateSecurityGroupPolicy",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "PrivateConnectivityCreateSecurityGroupTaggingPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "outposts:private-connectivity-resourceId"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPanoramaApplianceRolePolicy

Descrição: permite que o software de AWS IoT em um dispositivo AWS Panorama faça o upload de registros para a Amazon. CloudWatch

`AWSPanoramaApplianceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPanoramaApplianceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 01 de dezembro de 2020, 13:13 UTC
- Hora da edição: 01 de dezembro de 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*"
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPanoramaApplianceServiceRolePolicy

Descrição: permite que um dispositivo AWS Panorama faça upload de registros para a Amazon CloudWatch e obtenha objetos dos pontos de acesso do Amazon S3 criados para uso com AWS o Panorama.

`AWSPanoramaApplianceServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPanoramaApplianceServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 20 de outubro de 2021, 12:14 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDevicePutMetric",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "PanoramaDeviceMetrics"
        }
      }
    },
    {
      "Sid" : "PanoramaDeviceS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
```

```
        "s3:ListBucket",
        "s3:GetObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3:::*-nodepackage-store-*",
        "arn:aws:s3:::*-application-payload-store-*",
        "arn:aws:s3:*:*:accesspoint/panorama*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPanoramaFullAccess

Descrição: Fornece acesso total ao AWS Panorama

`AWSPanoramaFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPanoramaFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2020, 13:12 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC

- ARN: `arn:aws:iam::aws:policy/AWSPanoramaFullAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
```

```
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:panorama*",
        "arn:aws:secretsmanager:*:*:secret:Panorama*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "panorama.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
```

```
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "panorama.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPanoramaGreengrassGroupRolePolicy

Descrição: permite que uma função AWS Lambda em um dispositivo AWS Panorama gerencie recursos no Panorama, faça upload de registros e métricas para a Amazon CloudWatch e gerencie objetos em buckets criados para uso com o Panorama.

`AWSPanoramaGreengrassGroupRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPanoramaGreengrassGroupRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 01 de dezembro de 2020, 13:10 UTC
- Hora da edição: 06 de janeiro de 2021, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
```

```
        "s3:GetBucket*",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    },
    {
      "Sid" : "PanoramaCLoudWatchPutDashboard",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutDashboard",
      "Resource" : [
        "arn:aws:cloudwatch::*:dashboard/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaCloudWatchPutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "PanoramaGreenGrassCloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
    },
    {
      "Sid" : "PanoramaAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPanoramaSageMakerRolePolicy

Descrição: permite que SageMaker a Amazon gerencie objetos em buckets criados para uso com o AWS Panorama.

`AWSPanoramaSageMakerRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPanoramaSageMakerRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 01 de dezembro de 2020, 13:13 UTC
- Hora da edição: 01 de dezembro de 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPanoramaServiceLinkedRolePolicy

Descrição: Permite que o AWS Panorama gerencie recursos em AWS IoT, AWS Secrets Manager e AWS Panorama.

`AWSPanoramaServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 20 de outubro de 2021, 12:12 UTC
- Hora da edição: 20 de outubro de 2021, 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCertificateAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:AttachPrincipalPolicy",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreateCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreatePolicyAndVersionAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion",
        "iot:AttachPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeJobExecution",
        "iot:CreateJob",
        "iot:DeleteJob"
      ],
      "Resource" : [
```

```
        "arn:aws:iot:*:*:job/panorama*",
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:Describe*",
        "panorama:List*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:panorama*",
        "arn:aws:secretsmanager:*:*:secret:Panorama*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPanoramaServiceRolePolicy

Descrição: permite que o AWS Panorama gerencie recursos no Amazon S3, AWS IoT, AWS IoT GreenGrass, AWS Lambda SageMaker, Amazon e Amazon CloudWatch Logs e transfira funções de serviço para AWS IoT, AWS IoT e Amazon. GreenGrass SageMaker

`AWSPanoramaServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPanoramaServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 01 de dezembro de 2020, 13:14 UTC
- Hora da edição: 01 de dezembro de 2020, 13:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:AttachPrincipalPolicy",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreateCertificateAndPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreatePolicyVersionAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeJobExecution",
        "iot:CreateJob",
        "iot:DeleteJob"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/panorama*",
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:Describe*",
        "panorama:List*",
        "panorama:Get*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "PanoramaS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:DeleteBucket",
        "s3:ListBucket",
        "s3:GetBucket*",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIAMPassSageMakerRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaSageMakerRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaSageMakerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PanoramaIAMPassGreengrassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaGreengrassGroupRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassGroupRole",
        "arn:aws:iam::*:role/AWSPanoramaGreengrassRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassRole"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "greengrass.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PanoramaIAMPassIoTRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaApplianceRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaApplianceRole"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "iot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PanoramaGreenGrassAccess",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:AssociateRoleToGroup",
        "greengrass:AssociateServiceRoleToAccount",
        "greengrass:CreateResourceDefinition",
        "greengrass:CreateResourceDefinitionVersion",
        "greengrass:CreateCoreDefinition",
        "greengrass:CreateCoreDefinitionVersion",
        "greengrass:CreateDeployment",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:CreateGroup",
        "greengrass:CreateGroupCertificateAuthority",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateLoggerDefinition",
        "greengrass:CreateLoggerDefinitionVersion",
        "greengrass:CreateSubscriptionDefinition",
```

```
        "greengrass:CreateSubscriptionDefinitionVersion",
        "greengrass:DeleteCoreDefinition",
        "greengrass:DeleteFunctionDefinition",
        "greengrass:DeleteResourceDefinition",
        "greengrass:DeleteGroup",
        "greengrass:DeleteLoggerDefinition",
        "greengrass:DeleteSubscriptionDefinition",
        "greengrass:DisassociateRoleFromGroup",
        "greengrass:DisassociateServiceRoleFromAccount",
        "greengrass:GetAssociatedRole",
        "greengrass:GetConnectivityInfo",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetDeviceDefinition",
        "greengrass:GetDeviceDefinitionVersion",
        "greengrass:GetFunctionDefinition",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupCertificateAuthority",
        "greengrass:GetGroupCertificateConfiguration",
        "greengrass:GetGroupVersion",
        "greengrass:GetLoggerDefinition",
        "greengrass:GetLoggerDefinitionVersion",
        "greengrass:GetResourceDefinition",
        "greengrass:GetServiceRoleForAccount",
        "greengrass:GetSubscriptionDefinition",
        "greengrass:GetSubscriptionDefinitionVersion",
        "greengrass:ListCoreDefinitionVersions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeployments",
        "greengrass:ListDeviceDefinitionVersions",
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitionVersions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroupCertificateAuthorities",
        "greengrass:ListGroupVersions",
        "greengrass:ListGroups",
        "greengrass:ListLoggerDefinitionVersions",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListSubscriptionDefinitionVersions",
        "greengrass:ListSubscriptionDefinitions",
        "greengrass:ResetDeployments",
        "greengrass:UpdateConnectivityInfo",
```

```
        "greengrass:UpdateCoreDefinition",
        "greengrass:UpdateDeviceDefinition",
        "greengrass:UpdateFunctionDefinition",
        "greengrass:UpdateGroup",
        "greengrass:UpdateGroupCertificateConfiguration",
        "greengrass:UpdateLoggerDefinition",
        "greengrass:UpdateSubscriptionDefinition",
        "greengrass:UpdateResourceDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaLambdaUsersFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:CreateCompilationJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:StopCompilationJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/panorama*",
        "arn:aws:sagemaker:*:*:compilation-job/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerListAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:ListCompilationJobs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    },
    {
      "Sid" : "PanoramaCWLogsAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPolicy",
        "iot:CreateRoleAlias"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*",
        "arn:aws:iot:*:*:rolealias/panorama*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPartnerCentralChannelHandshakeApprovalManagement

Descrição: Fornece o acesso necessário para as atividades de gerenciamento de aprovação de handshake do canal.

`AWSPartnerCentralChannelHandshakeApprovalManagement` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPartnerCentralChannelHandshakeApprovalManagement` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 19 de novembro de 2025, 16:34 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralChannelHandshakeApprovalManagement`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ChannelHandshakeManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListChannelHandshakes",
```

```
        "partnercentral:AcceptChannelHandshake",
        "partnercentral:RejectChannelHandshake"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPartnerCentralChannelManagement

Descrição: Fornece o acesso necessário para as atividades de gerenciamento de canais.

`AWSPartnerCentralChannelManagement` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPartnerCentralChannelManagement` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 19 de novembro de 2025, 16:34 UTC
- Horário editado: 14 de fevereiro de 2026, 00:57 UTC

- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralChannelManagement`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ChannelManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateProgramManagementAccount",
        "partnercentral:UpdateProgramManagementAccount",
        "partnercentral:DeleteProgramManagementAccount",
        "partnercentral:ListProgramManagementAccounts",
        "partnercentral:GetProgramManagementAccount",
        "partnercentral:CreateRelationship",
        "partnercentral:UpdateRelationship",
        "partnercentral:DeleteRelationship",
        "partnercentral:GetRelationship",
        "partnercentral:ListRelationships",
        "partnercentral:CreateChannelHandshake",
        "partnercentral:AcceptChannelHandshake",
        "partnercentral:RejectChannelHandshake",
        "partnercentral:CancelChannelHandshake",
        "partnercentral:ListChannelHandshakes"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "ChannelBillingTransferRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferManagement",
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferReadOnly"
      ]
    },
    {
      "Sid" : "TaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/program-management-account/*",
        "arn:aws:partnercentral:*:*:catalog/*/channel-handshake/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "partnercentral-account-management:LegacyPartnerCentralRole" : "ChannelUser"
        }
      }
    },
    {
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartnerDashboard"
      ],
      "Resource" : [
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Resell_V1/Dashboard/*"
      ]
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPartnerCentralFullAccess

Descrição: Fornece acesso total ao AWS Partner Central e afins Serviços da AWS.

`AWSPartnerCentralFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPartnerCentralFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 18 de novembro de 2024, 23:33 UTC
- Horário editado: 12 de março de 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralFullAccess`

Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PassAWSPartnerCentralRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/PartnerCentralRoleFor*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "partnercentral-account-management.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PartnerUserRoleAssociation",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "Partnercentral-account-management:AssociatePartnerUser",
        "Partnercentral-account-management:DisassociatePartnerUser"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "VerificationAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "partnercentral:StartVerification",
        "partnercentral:GetVerification"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassAWSPartnerCentralSnapshotJobRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "resource-snapshot-job.partnercentral-
selling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerCentralMarketingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessMarketingCentral"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ChannelBillingTransferRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferManagement",
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferReadOnly"
      ]
    },
    {
      "Sid" : "PartnerCentralEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-
files/${aws:PrincipalAccount}/*"
    },
    {
      "Sid" : "SupportAccess",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeCases",
        "support:AddCommunicationToCase",
        "support:ResolveCase",
        "support:AddAttachmentsToSet",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListEntitiesAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeEntityAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Solution/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/OfferSet/*",
```

```
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAgreementsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerCentralAgentsSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:UseSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
```

```
        },
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPartnerCentralMarketingManagement

Descrição: Fornece o acesso necessário para atividades de marketing.

`AWSPartnerCentralMarketingManagement` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPartnerCentralMarketingManagement` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 01 de dezembro de 2025, 00:34 UTC
- Horário editado: 14 de fevereiro de 2026, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralMarketingManagement`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PartnerCentralMarketingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessMarketingCentral"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" :
 "MarketingStaff"
        }
      }
    },
    {
      "Sid" : "PartnerDiscoveryAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:SearchPartnerProfiles",
        "partnercentral:GetPartnerProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerProfileAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "partnercentral:StartProfileUpdateTask",
        "partnercentral:GetProfileUpdateTask",
        "partnercentral:CancelProfileUpdateTask",
        "partnercentral:PutProfileVisibility",
        "partnercentral:GetProfileVisibility"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/partner/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerCentralEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-
files/${aws:PrincipalAccount}/*"
    },
    {
```

```
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartnerDashboard"
      ],
      "Resource" : [
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/MarketingCampaign_V1/
Dashboard/*"
      ]
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPartnerCentralOpportunityManagement

Descrição: concede o acesso necessário para as atividades de gerenciamento de oportunidades.

`AWSPartnerCentralOpportunityManagement` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPartnerCentralOpportunityManagement` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 14 de novembro de 2024, 19:09 UTC
- Horário editado: 16 de junho de 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralOpportunityManagement`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OpportunityManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:AcceptEngagementInvitation",
        "partnercentral:AssignOpportunity",
        "partnercentral:AssociateOpportunity",
        "partnercentral:CreateEngagement",
        "partnercentral:CreateEngagementContext",
        "partnercentral:CreateEngagementInvitation",
        "partnercentral:CreateOpportunity",
        "partnercentral:CreateResourceSnapshot",
        "partnercentral:CreateResourceSnapshotJob",
        "partnercentral:DeleteResourceSnapshotJob",
        "partnercentral:DisassociateOpportunity",
```

```
        "partnercentral:GetAwsOpportunitySummary",
        "partnercentral:GetEngagement",
        "partnercentral:GetEngagementInvitation",
        "partnercentral:GetOpportunity",
        "partnercentral:GetProspectingFromEngagementTask",
        "partnercentral:GetResourceSnapshot",
        "partnercentral:GetResourceSnapshotJob",
        "partnercentral:ListEngagementByAcceptingInvitationTasks",
        "partnercentral:ListEngagementFromOpportunityTasks",
        "partnercentral:ListEngagementInvitations",
        "partnercentral:ListEngagementMembers",
        "partnercentral:ListEngagementResourceAssociations",
        "partnercentral:ListEngagements",
        "partnercentral:ListOpportunities",
        "partnercentral:ListOpportunityFromEngagementTasks",
        "partnercentral:ListProspectingFromEngagementTasks",
        "partnercentral:ListResourceSnapshotJobs",
        "partnercentral:ListResourceSnapshots",
        "partnercentral:ListSolutions",
        "partnercentral:RejectEngagementInvitation",
        "partnercentral:StartEngagementByAcceptingInvitationTask",
        "partnercentral:StartEngagementFromOpportunityTask",
        "partnercentral:StartOpportunityFromEngagementTask",
        "partnercentral:StartProspectingFromEngagementTask",
        "partnercentral:StartResourceSnapshotJob",
        "partnercentral:StopResourceSnapshotJob",
        "partnercentral:SubmitOpportunity",
        "partnercentral:UpdateEngagementContext",
        "partnercentral:UpdateOpportunity"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "ListingAWSMarketplaceEntities",
      "Effect" : "Allow",
      "Action" : [
```

```
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceEntityAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Solution/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/OfferSet/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" : "AceManager"
        }
      }
    },
    {
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartnerDashboard"
      ],
      "Resource" : [
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Opportunity_V1/Dashboard/
*",
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Engagement_V1/Dashboard/*"
      ]
    },
    {
      "Sid" : "CollaborationChannelAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "partnercentral:CreateCollaborationChannelRequest",
        "partnercentral:ListCollaborationChannels",
        "partnercentral:GetCollaborationChannel",
        "partnercentral:CreateCollaborationChannelMembers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "TaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/opportunity/*",
        "arn:aws:partnercentral:*:*:catalog/*/resource-snapshot-job/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerCentralAgentsSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:UseSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        },
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPartnerCentralRevenueAttributionManagement

Descrição: Fornece o acesso necessário para atividades de gerenciamento de atribuição de receita.

`AWSPartnerCentralRevenueAttributionManagement` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPartnerCentralRevenueAttributionManagement` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 30 de junho de 2026, 19:12 UTC
- Horário editado: 30 de junho de 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralRevenueAttributionManagement`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RevenueMeasurementCreation",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateRevenueAttribution",
        "partnercentral:CreateMarketplaceRevenueShare",
        "partnercentral:CreateMarketplaceRevenueShareAllocation"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "RevenueMeasurementListing",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListRevenueAttributions",
        "partnercentral:ListRevenueAttributionAllocations",
        "partnercentral:ListMarketplaceRevenueShares",
        "partnercentral:ListMarketplaceRevenueShareAllocations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "RevenueAttributionManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetRevenueAttribution",
        "partnercentral:UpdateRevenueAttribution",
        "partnercentral:GetRevenueAttributionAllocation",
        "partnercentral:StartRevenueAttributionAllocationsTask",
        "partnercentral:GetRevenueAttributionAllocationsTask"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/revenue-attribution/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
```

```
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "MarketplaceRevenueShareManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetMarketplaceRevenueShare",
        "partnercentral:GetMarketplaceRevenueShareAllocation",
        "partnercentral:UpdateMarketplaceRevenueShareAllocation"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/marketplace-revenue-share/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "TaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/revenue-attribution/*",
        "arn:aws:partnercentral:*:*:catalog/*/marketplace-revenue-share/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "OpportunityListing",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListOpportunities"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "OpportunityAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetOpportunity"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/opportunity/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerListing",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
```

```
        ]
      }
    }
  },
  {
    "Sid" : "PartnerResourceAccess",
    "Effect" : "Allow",
    "Action" : [
      "partnercentral:GetPartner"
    ],
    "Resource" : "arn:aws:partnercentral:*:*:catalog/*/partner/*",
    "Condition" : {
      "StringEquals" : {
        "partnercentral:Catalog" : [
          "AWS",
          "Sandbox"
        ]
      }
    }
  },
  {
    "Sid" : "ListingAWSMarketplaceEntities",
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:ListEntities"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AWSMarketplaceEntityAccess",
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:DescribeEntity"
    ],
    "Resource" : [
      "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
    ]
  },
  {
    "Sid" : "AmazonQPartnerAssistantAccess",
    "Effect" : "Allow",
    "Action" : [
      "q:StartConversation",
      "q:SendMessage",
```

```
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPartnerCentralSandboxFullAccess

Descrição: concede o acesso necessário para testes de desenvolvedores no catálogo do sandbox.

`AWSPartnerCentralSandboxFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPartnerCentralSandboxFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 14 de novembro de 2024, 19:10 UTC
- Horário editado: 12 de março de 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralSandboxFullAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSPartnerCentralSandboxAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : "Sandbox"
        }
      }
    },
    {
      "Sid" : "PartnerCentralAgentsSandboxSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:UseSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : "Sandbox"
        },
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    },
    {
      "Sid" : "PassAWSPartnerCentralSnapshotJobRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "resource-snapshot-job.partnercentral-
selling.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy

Descrição: Fornece acesso ao ResourceSnapshotJob para ler um recurso e capturá-lo no contrato de destino.

`AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Horário de criação: 10 de dezembro de 2024, 18:21 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateResourceSnapshot"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*::catalog/AWS/engagement/*",
        "arn:aws:partnercentral:*::catalog/Sandbox/engagement/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetOpportunity"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/AWS/opportunity/*",
        "arn:aws:partnercentral:*:*:catalog/Sandbox/opportunity/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPartnerLedSupportReadOnlyAccess

Descrição: essa política pode ser usada para conceder acesso somente de leitura às APIs que podem ler metadados de serviço para serviços em sua Conta da AWS. Você pode usar essa política para fornecer aos seus parceiros do Programa de Partner-Led Suporte acesso aos serviços especificados na seção de detalhes das permissões abaixo.

`AWSPartnerLedSupportReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPartnerLedSupportReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 22 de novembro de 2024, 20:06 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerLedSupportReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
```

```
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:describeCertificateAuthority",
        "acm-pca:describeCertificateAuthorityAuditReport",
        "acm-pca:getCertificate",
        "acm-pca:getCertificateAuthorityCertificate",
        "acm-pca:getCertificateAuthorityCsr",
        "acm-pca:listCertificateAuthorities",
        "acm-pca:listTags",
        "acm:describeCertificate",
        "acm:getAccountConfiguration",
        "acm:getCertificate",
        "acm:listCertificates",
        "acm:listTagsForCertificate",
        "athena:batchGetNamedQuery",
        "athena:batchGetQueryExecution",
        "athena:getCalculationExecution",
        "athena:getCalculationExecutionStatus",
        "athena:getDataCatalog",
        "athena:getNamedQuery",
        "athena:getNotebookMetadata",
        "athena:getQueryExecution",
        "athena:getQueryRuntimeStatistics",
        "athena:getSession",
```

```
        "athena:getSessionStatus",
        "athena:getWorkGroup",
        "athena:listApplicationDPUSizes",
        "athena:listCalculationExecutions",
        "athena:listDataCatalogs",
        "athena:listEngineVersions",
        "athena:listExecutors",
        "athena:listNamedQueries",
        "athena:listNotebookMetadata",
        "athena:listNotebookSessions",
        "athena:listQueryExecutions",
        "athena:listSessions",
        "athena:listTagsForResource",
        "athena:listWorkGroups",
        "backup-gateway:getGateway",
        "backup-gateway:getHypervisor",
        "backup-gateway:getHypervisorPropertyMappings",
        "backup-gateway:getVirtualMachine",
        "backup-gateway:listGateways",
        "backup-gateway:listHypervisors",
        "backup-gateway:listVirtualMachines",
        "backup:describeBackupJob",
        "backup:describeBackupVault",
        "backup:describeCopyJob",
        "backup:describeFramework",
        "backup:describeGlobalSettings",
        "backup:describeProtectedResource",
        "backup:describeRecoveryPoint",
        "backup:describeRegionSettings",
        "backup:describeReportJob",
        "backup:describeReportPlan",
        "backup:describeRestoreJob",
        "backup:getBackupPlan",
        "backup:getBackupPlanFromJSON",
        "backup:getBackupPlanFromTemplate",
        "backup:getBackupSelection",
        "backup:getBackupVaultAccessPolicy",
        "backup:getBackupVaultNotifications",
        "backup:getLegalHold",
        "backup:getRecoveryPointRestoreMetadata",
        "backup:getRestoreJobMetadata",
        "backup:getRestoreTestingInferredMetadata",
        "backup:getRestoreTestingPlan",
        "backup:getRestoreTestingSelection",
```

```
        "backup:getSupportedResourceTypes",
        "backup:listBackupJobs",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "backup:listBackupPlans",
        "backup:listBackupSelections",
        "backup:listBackupVaults",
        "backup:listCopyJobs",
        "backup:listFrameworks",
        "backup:listLegalHolds",
        "backup:listProtectedResources",
        "backup:listRecoveryPointsByBackupVault",
        "backup:listRecoveryPointsByLegalHold",
        "backup:listRecoveryPointsByResource",
        "backup:listReportJobs",
        "backup:listReportPlans",
        "backup:listRestoreJobs",
        "backup:listRestoreJobsByProtectedResource",
        "backup:listRestoreTestingPlans",
        "backup:listRestoreTestingSelections",
        "backup:listTags",
        "cloudformation:batchDescribeTypeConfigurations",
        "cloudformation:describeAccountLimits",
        "cloudformation:describeChangeSet",
        "cloudformation:describeChangeSetHooks",
        "cloudformation:describePublisher",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
        "cloudformation:describeStackResource",
        "cloudformation:describeStackResources",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeStacks",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
        "cloudformation:estimateTemplateCost",
        "cloudformation:getStackPolicy",
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
```

```
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
        "cloudformation:listStackSets",
        "cloudformation:listStacks",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypeVersions",
        "cloudformation:listTypes",
        "cloudfront:describeFunction",
        "cloudfront:getCachePolicy",
        "cloudfront:getCachePolicyConfig",
        "cloudfront:getCloudFrontOriginAccessIdentity",
        "cloudfront:getCloudFrontOriginAccessIdentityConfig",
        "cloudfront:getContinuousDeploymentPolicy",
        "cloudfront:getContinuousDeploymentPolicyConfig",
        "cloudfront:getDistribution",
        "cloudfront:getDistributionConfig",
        "cloudfront:getInvalidation",
        "cloudfront:getKeyGroup",
        "cloudfront:getKeyGroupConfig",
        "cloudfront:getMonitoringSubscription",
        "cloudfront:getOriginAccessControl",
        "cloudfront:getOriginAccessControlConfig",
        "cloudfront:getOriginRequestPolicy",
        "cloudfront:getOriginRequestPolicyConfig",
        "cloudfront:getPublicKey",
        "cloudfront:getPublicKeyConfig",
        "cloudfront:getRealtimeLogConfig",
        "cloudfront:getResponseHeadersPolicy",
        "cloudfront:getResponseHeadersPolicyConfig",
        "cloudfront:getStreamingDistribution",
        "cloudfront:getStreamingDistributionConfig",
        "cloudfront:listCachePolicies",
        "cloudfront:listCloudFrontOriginAccessIdentities",
        "cloudfront:listContinuousDeploymentPolicies",
        "cloudfront:listDistributions",
        "cloudfront:listDistributionsByCachePolicyId",
        "cloudfront:listDistributionsByKeyGroup",
        "cloudfront:listDistributionsByOriginRequestPolicyId",
        "cloudfront:listDistributionsByRealtimeLogConfig",
        "cloudfront:listDistributionsByResponseHeadersPolicyId",
        "cloudfront:listDistributionsByWebACLId",
        "cloudfront:listFunctions",
        "cloudfront:listInvalidations",
        "cloudfront:listKeyGroups",
```

```
        "cloudfront:listOriginAccessControls",
        "cloudfront:listOriginRequestPolicies",
        "cloudfront:listPublicKeys",
        "cloudfront:listRealtimeLogConfigs",
        "cloudfront:listResponseHeadersPolicies",
        "cloudfront:listStreamingDistributions",
        "cloudtrail:describeTrails",
        "cloudtrail:getEventSelectors",
        "cloudtrail:lookupEvents",
        "cloudwatch:describeAlarmHistory",
        "cloudwatch:describeAlarms",
        "cloudwatch:describeAlarmsForMetric",
        "cloudwatch:describeAnomalyDetectors",
        "cloudwatch:describeInsightRules",
        "cloudwatch:getDashboard",
        "cloudwatch:getInsightRuleReport",
        "cloudwatch:getMetricData",
        "cloudwatch:getMetricStatistics",
        "cloudwatch:getMetricStream",
        "cloudwatch:listDashboards",
        "cloudwatch:listManagedInsightRules",
        "cloudwatch:listMetricStreams",
        "cloudwatch:listMetrics",
        "codepipeline:getPipeline",
        "codepipeline:getPipelineState",
        "codepipeline:listActionTypes",
        "codepipeline:listPipelineExecutions",
        "codepipeline:listPipelines",
        "cognito-identity:describeIdentityPool",
        "cognito-identity:getIdentityPoolRoles",
        "cognito-identity:listIdentities",
        "cognito-identity:listIdentityPools",
        "cognito-idp:describeIdentityProvider",
        "cognito-idp:describeResourceServer",
        "cognito-idp:describeRiskConfiguration",
        "cognito-idp:describeUserImportJob",
        "cognito-idp:describeUserPool",
        "cognito-idp:describeUserPoolClient",
        "cognito-idp:describeUserPoolDomain",
        "cognito-idp:getGroup",
        "cognito-idp:getUICustomization",
        "cognito-idp:getUserPoolMfaConfig",
        "cognito-idp:listGroups",
        "cognito-idp:listIdentityProviders",
```

```
        "cognito-idp:listResourceServers",
        "cognito-idp:listUserImportJobs",
        "cognito-idp:listUserPoolClients",
        "cognito-idp:listUserPools",
        "cognito-sync:describeDataset",
        "cognito-sync:describeIdentityPoolUsage",
        "cognito-sync:describeIdentityUsage",
        "cognito-sync:getCognitoEvents",
        "cognito-sync:getIdentityPoolConfiguration",
        "cognito-sync:listDatasets",
        "cognito-sync:listIdentityPoolUsage",
        "connect:describeContact",
        "connect:describePhoneNumber",
        "connect:describeQuickConnect",
        "connect:describeUser",
        "connect:getCurrentMetricData",
        "connect:getMetricData",
        "connect:listContactEvaluations",
        "connect:listEvaluationFormVersions",
        "connect:listEvaluationForms",
        "connect:listPhoneNumbersV2",
        "connect:listQuickConnects",
        "connect:listRoutingProfiles",
        "connect:listSecurityProfiles",
        "connect:listUsers",
        "connect:listViewVersions",
        "connect:listViews",
        "directconnect:describeConnectionLoa",
        "directconnect:describeConnections",
        "directconnect:describeConnectionsOnInterconnect",
        "directconnect:describeCustomerMetadata",
        "directconnect:describeDirectConnectGatewayAssociationProposals",
        "directconnect:describeDirectConnectGatewayAssociations",
        "directconnect:describeDirectConnectGatewayAttachments",
        "directconnect:describeDirectConnectGateways",
        "directconnect:describeHostedConnections",
        "directconnect:describeInterconnectLoa",
        "directconnect:describeInterconnects",
        "directconnect:describeLags",
        "directconnect:describeLoa",
        "directconnect:describeLocations",
        "directconnect:describeRouterConfiguration",
        "directconnect:describeVirtualGateways",
        "directconnect:describeVirtualInterfaces",
```

```
        "dms:describeAccountAttributes",
        "dms:describeApplicableIndividualAssessments",
        "dms:describeConnections",
        "dms:describeEndpointSettings",
        "dms:describeEndpointTypes",
        "dms:describeEndpoints",
        "dms:describeEventCategories",
        "dms:describeEventSubscriptions",
        "dms:describeEvents",
        "dms:describeFleetAdvisorCollectors",
        "dms:describeFleetAdvisorDatabases",
        "dms:describeFleetAdvisorLsaAnalysis",
        "dms:describeFleetAdvisorSchemaObjectSummary",
        "dms:describeFleetAdvisorSchemas",
        "dms:describeOrderableReplicationInstances",
        "dms:describePendingMaintenanceActions",
        "dms:describeRefreshSchemasStatus",
        "dms:describeReplicationInstanceTaskLogs",
        "dms:describeReplicationInstances",
        "dms:describeReplicationSubnetGroups",
        "dms:describeReplicationTaskAssessmentResults",
        "dms:describeReplicationTaskAssessmentRuns",
        "dms:describeReplicationTaskIndividualAssessments",
        "dms:describeReplicationTasks",
        "dms:describeSchemas",
        "dms:describeTableStatistics",
        "ds:describeClientAuthenticationSettings",
        "ds:describeConditionalForwarders",
        "ds:describeDirectories",
        "ds:describeDomainControllers",
        "ds:describeEventTopics",
        "ds:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
        "ds:getSnapshotLimits",
        "ds:listIpRoutes",
        "ds:listSchemaExtensions",
        "ds:listTagsForResource",
        "ec2:describeAccountAttributes",
        "ec2:describeAddressTransfers",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
```

```
        "ec2:describeAggregateIdFormat",
        "ec2:describeAvailabilityZones",
        "ec2:describeBundleTasks",
        "ec2:describeByoipCidrs",
        "ec2:describeCapacityReservationFleets",
        "ec2:describeCapacityReservations",
        "ec2:describeCarrierGateways",
        "ec2:describeClassicLinkInstances",
        "ec2:describeClientVpnAuthorizationRules",
        "ec2:describeClientVpnConnections",
        "ec2:describeClientVpnEndpoints",
        "ec2:describeClientVpnRoutes",
        "ec2:describeClientVpnTargetNetworks",
        "ec2:describeCoipPools",
        "ec2:describeConversionTasks",
        "ec2:describeCustomerGateways",
        "ec2:describeDhcpOptions",
        "ec2:describeEgressOnlyInternetGateways",
        "ec2:describeExportImageTasks",
        "ec2:describeExportTasks",
        "ec2:describeFastLaunchImages",
        "ec2:describeFastSnapshotRestores",
        "ec2:describeFleetHistory",
        "ec2:describeFleetInstances",
        "ec2:describeFleets",
        "ec2:describeFlowLogs",
        "ec2:describeFpgaImageAttribute",
        "ec2:describeFpgaImages",
        "ec2:describeHostReservationOfferings",
        "ec2:describeHostReservations",
        "ec2:describeHosts",
        "ec2:describeIamInstanceProfileAssociations",
        "ec2:describeIdFormat",
        "ec2:describeIdentityIdFormat",
        "ec2:describeImageAttribute",
        "ec2:describeImages",
        "ec2:describeImportImageTasks",
        "ec2:describeImportSnapshotTasks",
        "ec2:describeInstanceAttribute",
        "ec2:describeInstanceCreditSpecifications",
        "ec2:describeInstanceEventNotificationAttributes",
        "ec2:describeInstanceEventWindows",
        "ec2:describeInstanceStatus",
        "ec2:describeInstanceTypeOfferings",
```

```
        "ec2:describeInstanceTypes",
        "ec2:describeInstances",
        "ec2:describeInternetGateways",
        "ec2:describeIpamPools",
        "ec2:describeIpamScopes",
        "ec2:describeIpams",
        "ec2:describeIpv6Pools",
        "ec2:describeKeyPairs",
        "ec2:describeLaunchTemplateVersions",
        "ec2:describeLaunchTemplates",
        "ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:describeLocalGatewayRouteTableVpcAssociations",
        "ec2:describeLocalGatewayRouteTables",
        "ec2:describeLocalGatewayVirtualInterfaceGroups",
        "ec2:describeLocalGatewayVirtualInterfaces",
        "ec2:describeLocalGateways",
        "ec2:describeManagedPrefixLists",
        "ec2:describeMovingAddresses",
        "ec2:describeNatGateways",
        "ec2:describeNetworkAcls",
        "ec2:describeNetworkInterfaceAttribute",
        "ec2:describeNetworkInterfaces",
        "ec2:describePlacementGroups",
        "ec2:describePrefixLists",
        "ec2:describePrincipalIdFormat",
        "ec2:describePublicIpv4Pools",
        "ec2:describeRegions",
        "ec2:describeReservedInstances",
        "ec2:describeReservedInstancesListings",
        "ec2:describeReservedInstancesModifications",
        "ec2:describeReservedInstancesOfferings",
        "ec2:describeRouteTables",
        "ec2:describeScheduledInstanceAvailability",
        "ec2:describeScheduledInstances",
        "ec2:describeSecurityGroupReferences",
        "ec2:describeSecurityGroupRules",
        "ec2:describeSecurityGroups",
        "ec2:describeSnapshotAttribute",
        "ec2:describeSnapshotTierStatus",
        "ec2:describeSnapshots",
        "ec2:describeSpotDatafeedSubscription",
        "ec2:describeSpotFleetInstances",
        "ec2:describeSpotFleetRequestHistory",
        "ec2:describeSpotFleetRequests",
```

```
        "ec2:describeSpotInstanceRequests",
        "ec2:describeSpotPriceHistory",
        "ec2:describeStaleSecurityGroups",
        "ec2:describeStoreImageTasks",
        "ec2:describeSubnets",
        "ec2:describeTags",
        "ec2:describeTrafficMirrorFilters",
        "ec2:describeTrafficMirrorSessions",
        "ec2:describeTrafficMirrorTargets",
        "ec2:describeTransitGatewayAttachments",
        "ec2:describeTransitGatewayConnectPeers",
        "ec2:describeTransitGatewayMulticastDomains",
        "ec2:describeTransitGatewayPeeringAttachments",
        "ec2:describeTransitGatewayPolicyTables",
        "ec2:describeTransitGatewayRouteTableAnnouncements",
        "ec2:describeTransitGatewayRouteTables",
        "ec2:describeTransitGatewayVpcAttachments",
        "ec2:describeTransitGateways",
        "ec2:describeVerifiedAccessEndpoints",
        "ec2:describeVerifiedAccessGroups",
        "ec2:describeVerifiedAccessInstances",
        "ec2:describeVerifiedAccessTrustProviders",
        "ec2:describeVolumeAttribute",
        "ec2:describeVolumeStatus",
        "ec2:describeVolumes",
        "ec2:describeVolumesModifications",
        "ec2:describeVpcAttribute",
        "ec2:describeVpcClassicLink",
        "ec2:describeVpcClassicLinkDnsSupport",
        "ec2:describeVpcEndpointConnectionNotifications",
        "ec2:describeVpcEndpointConnections",
        "ec2:describeVpcEndpointServiceConfigurations",
        "ec2:describeVpcEndpointServicePermissions",
        "ec2:describeVpcEndpointServices",
        "ec2:describeVpcEndpoints",
        "ec2:describeVpcPeeringConnections",
        "ec2:describeVpcs",
        "ec2:describeVpnConnections",
        "ec2:describeVpnGateways",
        "ec2:getAssociatedIpv6PoolCidrs",
        "ec2:getCapacityReservationUsage",
        "ec2:getCoipPoolUsage",
        "ec2:getConsoleOutput",
        "ec2:getConsoleScreenshot",
```

```
        "ec2:getDefaultCreditSpecification",
        "ec2:getEbsDefaultKmsKeyId",
        "ec2:getEbsEncryptionByDefault",
        "ec2:getGroupsForCapacityReservation",
        "ec2:getHostReservationPurchasePreview",
        "ec2:getInstanceTypesFromInstanceRequirements",
        "ec2:getIpamAddressHistory",
        "ec2:getIpamPoolAllocations",
        "ec2:getIpamPoolCidrs",
        "ec2:getIpamResourceCidrs",
        "ec2:getLaunchTemplateData",
        "ec2:getManagedPrefixListAssociations",
        "ec2:getManagedPrefixListEntries",
        "ec2:getReservedInstancesExchangeQuote",
        "ec2:getSerialConsoleAccessStatus",
        "ec2:getSpotPlacementScores",
        "ec2:getSubnetCidrReservations",
        "ec2:getTransitGatewayMulticastDomainAssociations",
        "ec2:getTransitGatewayPrefixListReferences",
        "ec2:getVerifiedAccessEndpointPolicy",
        "ec2:getVerifiedAccessGroupPolicy",
        "ec2:listImagesInRecycleBin",
        "ec2:listSnapshotsInRecycleBin",
        "ec2:searchLocalGatewayRoutes",
        "ec2:searchTransitGatewayMulticastGroups",
        "ec2:searchTransitGatewayRoutes",
        "ecs:describeCapacityProviders",
        "ecs:describeClusters",
        "ecs:describeContainerInstances",
        "ecs:describeServices",
        "ecs:describeTaskDefinition",
        "ecs:describeTaskSets",
        "ecs:describeTasks",
        "ecs:getTaskProtection",
        "ecs:listAccountSettings",
        "ecs:listAttributes",
        "ecs:listClusters",
        "ecs:listContainerInstances",
        "ecs:listServices",
        "ecs:listServicesByNamespace",
        "ecs:listTagsForResource",
        "ecs:listTaskDefinitionFamilies",
        "ecs:listTaskDefinitions",
        "ecs:listTasks",
```

```
        "eks:describeAccessEntry",
        "eks:describeAddon",
        "eks:describeAddonConfiguration",
        "eks:describeAddonVersions",
        "eks:describeCluster",
        "eks:describeEksAnywhereSubscription",
        "eks:describeFargateProfile",
        "eks:describeIdentityProviderConfig",
        "eks:describeNodegroup",
        "eks:describePodIdentityAssociation",
        "eks:describeUpdate",
        "eks:listAccessEntries",
        "eks:listAccessPolicies",
        "eks:listAddons",
        "eks:listAssociatedAccessPolicies",
        "eks:listClusters",
        "eks:listEksAnywhereSubscriptions",
        "eks:listFargateProfiles",
        "eks:listIdentityProviderConfigs",
        "eks:listNodegroups",
        "eks:listPodIdentityAssociations",
        "eks:listUpdates",
        "elasticache:describeCacheClusters",
        "elasticache:describeCacheEngineVersions",
        "elasticache:describeCacheParameterGroups",
        "elasticache:describeCacheParameters",
        "elasticache:describeCacheSecurityGroups",
        "elasticache:describeCacheSubnetGroups",
        "elasticache:describeEngineDefaultParameters",
        "elasticache:describeEvents",
        "elasticache:describeGlobalReplicationGroups",
        "elasticache:describeReplicationGroups",
        "elasticache:describeReservedCacheNodes",
        "elasticache:describeReservedCacheNodesOfferings",
        "elasticache:describeServerlessCacheSnapshots",
        "elasticache:describeServerlessCaches",
        "elasticache:describeServiceUpdates",
        "elasticache:describeSnapshots",
        "elasticache:describeUpdateActions",
        "elasticache:describeUserGroups",
        "elasticache:describeUsers",
        "elasticache:listAllowedNodeTypeModifications",
        "elasticache:listTagsForResource",
        "elasticbeanstalk:checkDNSAvailability",
```

```
        "elasticbeanstalk:describeAccountAttributes",
        "elasticbeanstalk:describeApplicationVersions",
        "elasticbeanstalk:describeApplications",
        "elasticbeanstalk:describeConfigurationOptions",
        "elasticbeanstalk:describeEnvironmentHealth",
        "elasticbeanstalk:describeEnvironmentManagedActionHistory",
        "elasticbeanstalk:describeEnvironmentManagedActions",
        "elasticbeanstalk:describeEnvironmentResources",
        "elasticbeanstalk:describeEnvironments",
        "elasticbeanstalk:describeEvents",
        "elasticbeanstalk:describeInstancesHealth",
        "elasticbeanstalk:describePlatformVersion",
        "elasticbeanstalk:listAvailableSolutionStacks",
        "elasticbeanstalk:listPlatformBranches",
        "elasticbeanstalk:listPlatformVersions",
        "elasticbeanstalk:validateConfigurationSettings",
        "elasticfilesystem:describeAccessPoints",
        "elasticfilesystem:describeFileSystemPolicy",
        "elasticfilesystem:describeFileSystems",
        "elasticfilesystem:describeLifecycleConfiguration",
        "elasticfilesystem:describeMountTargetSecurityGroups",
        "elasticfilesystem:describeMountTargets",
        "elasticfilesystem:describeTags",
        "elasticfilesystem:listTagsForResource",
        "elasticloadbalancing:describeAccountLimits",
        "elasticloadbalancing:describeInstanceHealth",
        "elasticloadbalancing:describeListenerCertificates",
        "elasticloadbalancing:describeListeners",
        "elasticloadbalancing:describeLoadBalancerAttributes",
        "elasticloadbalancing:describeLoadBalancerPolicies",
        "elasticloadbalancing:describeLoadBalancerPolicyTypes",
        "elasticloadbalancing:describeLoadBalancers",
        "elasticloadbalancing:describeRules",
        "elasticloadbalancing:describeSSLPolicies",
        "elasticloadbalancing:describeTags",
        "elasticloadbalancing:describeTargetGroupAttributes",
        "elasticloadbalancing:describeTargetGroups",
        "elasticloadbalancing:describeTargetHealth",
        "elasticloadbalancing:describeTrustStoreAssociations",
        "elasticloadbalancing:describeTrustStoreRevocations",
        "elasticloadbalancing:describeTrustStores",
        "emr-containers:describeJobRun",
        "emr-containers:describeJobTemplate",
        "emr-containers:describeManagedEndpoint",
```

```
        "emr-containers:describeVirtualCluster",
        "emr-containers:listJobRuns",
        "emr-containers:listJobTemplates",
        "emr-containers:listManagedEndpoints",
        "emr-containers:listVirtualClusters",
        "emr-serverless:getApplication",
        "emr-serverless:getJobRun",
        "emr-serverless:listApplications",
        "es:describeDomain",
        "es:describeDomainAutoTunes",
        "es:describeDomainChangeProgress",
        "es:describeDomainConfig",
        "es:describeDomains",
        "es:describeDryRunProgress",
        "es:describeElasticsearchDomain",
        "es:describeElasticsearchDomainConfig",
        "es:describeElasticsearchDomains",
        "es:describeInboundConnections",
        "es:describeInstanceTypeLimits",
        "es:describeOutboundConnections",
        "es:describePackages",
        "es:describeReservedInstanceOfferings",
        "es:describeReservedInstances",
        "es:describeVpcEndpoints",
        "es:getCompatibleVersions",
        "es:getPackageVersionHistory",
        "es:getUpgradeHistory",
        "es:getUpgradeStatus",
        "es:listDomainNames",
        "es:listDomainsForPackage",
        "es:listInstanceTypeDetails",
        "es:listPackagesForDomain",
        "es:listScheduledActions",
        "es:listTags",
        "es:listVersions",
        "es:listVpcEndpointAccess",
        "es:listVpcEndpoints",
        "es:listVpcEndpointsForDomain",
        "events:describeApiDestination",
        "events:describeArchive",
        "events:describeConnection",
        "events:describeEndpoint",
        "events:describeEventBus",
        "events:describeEventSource",
```

```
        "events:describePartnerEventSource",
        "events:describeReplay",
        "events:describeRule",
        "events:listApiDestinations",
        "events:listArchives",
        "events:listConnections",
        "events:listEndpoints",
        "events:listEventBuses",
        "events:listEventSources",
        "events:listPartnerEventSourceAccounts",
        "events:listPartnerEventSources",
        "events:listReplays",
        "events:listRuleNamesByTarget",
        "events:listRules",
        "events:listTargetsByRule",
        "events:testEventPattern",
        "fsx:describeBackups",
        "fsx:describeDataRepositoryAssociations",
        "fsx:describeDataRepositoryTasks",
        "fsx:describeFileCaches",
        "fsx:describeFileSystems",
        "fsx:describeSnapshots",
        "fsx:describeStorageVirtualMachines",
        "fsx:describeVolumes",
        "fsx:listTagsForResource",
        "glue:batchGetBlueprints",
        "glue:batchGetCrawlers",
        "glue:batchGetDevEndpoints",
        "glue:batchGetJobs",
        "glue:batchGetPartition",
        "glue:batchGetTriggers",
        "glue:batchGetWorkflows",
        "glue:checkSchemaVersionValidity",
        "glue:getBlueprint",
        "glue:getBlueprintRun",
        "glue:getBlueprintRuns",
        "glue:getCatalogImportStatus",
        "glue:getClassifier",
        "glue:getClassifiers",
        "glue:getColumnStatisticsForPartition",
        "glue:getColumnStatisticsForTable",
        "glue:getCrawler",
        "glue:getCrawlerMetrics",
        "glue:getCrawlers",
```

```
        "glue:getCustomEntityType",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
        "glue:getDataQualityRuleset",
        "glue:getDataQualityRulesetEvaluationRun",
        "glue:getDatabase",
        "glue:getDatabases",
        "glue:getDataflowGraph",
        "glue:getDevEndpoint",
        "glue:getDevEndpoints",
        "glue:getJob",
        "glue:getJobRun",
        "glue:getJobRuns",
        "glue:getJobs",
        "glue:getMLTaskRun",
        "glue:getMLTaskRuns",
        "glue:getMLTransform",
        "glue:getMLTransforms",
        "glue:getMapping",
        "glue:getPartition",
        "glue:getPartitionIndexes",
        "glue:getPartitions",
        "glue:getRegistry",
        "glue:getResourcePolicies",
        "glue:getResourcePolicy",
        "glue:getSchema",
        "glue:getSchemaByDefinition",
        "glue:getSchemaVersion",
        "glue:getSchemaVersionsDiff",
        "glue:getSession",
        "glue:getStatement",
        "glue:getTable",
        "glue:getTableVersions",
        "glue:getTables",
        "glue:getTrigger",
        "glue:getTriggers",
        "glue:getUserDefinedFunction",
        "glue:getUserDefinedFunctions",
        "glue:getWorkflow",
        "glue:getWorkflowRun",
        "glue:getWorkflowRuns",
        "glue:listCrawlers",
        "glue:listCrawls",
        "glue:listDataQualityResults",
```

```
        "glue:listDataQualityRuleRecommendationRuns",
        "glue:listDataQualityRulesetEvaluationRuns",
        "glue:listDataQualityRulesets",
        "glue:listDevEndpoints",
        "glue:listMLTransforms",
        "glue:listRegistries",
        "glue:listSchemaVersions",
        "glue:listSchemas",
        "glue:listSessions",
        "glue:listStatements",
        "glue:querySchemaVersionMetadata",
        "guardduty:getFindings",
        "guardduty:listDetectors",
        "guardduty:listFindings",
        "guardduty:listIPSets",
        "guardduty:listThreatIntelSets",
        "iam:getAccessKeyLastUsed",
        "iam:getAccountAuthorizationDetails",
        "iam:getAccountPasswordPolicy",
        "iam:getAccountSummary",
        "iam:getContextKeysForCustomPolicy",
        "iam:getContextKeysForPrincipalPolicy",
        "iam:getCredentialReport",
        "iam:getGroup",
        "iam:getGroupPolicy",
        "iam:getInstanceProfile",
        "iam:getLoginProfile",
        "iam:getOpenIDConnectProvider",
        "iam:getPolicy",
        "iam:getPolicyVersion",
        "iam:getRole",
        "iam:getRolePolicy",
        "iam:getSAMLProvider",
        "iam:getSSHPublicKey",
        "iam:getServerCertificate",
        "iam:getServiceLinkedRoleDeletionStatus",
        "iam:getUser",
        "iam:getUserPolicy",
        "iam:listAccessKeys",
        "iam:listAccountAliases",
        "iam:listAttachedGroupPolicies",
        "iam:listAttachedRolePolicies",
        "iam:listAttachedUserPolicies",
        "iam:listEntitiesForPolicy",
```

```
        "iam:listGroupPolicies",
        "iam:listGroups",
        "iam:listGroupsForUser",
        "iam:listInstanceProfiles",
        "iam:listInstanceProfilesForRole",
        "iam:listMFADevices",
        "iam:listOpenIDConnectProviders",
        "iam:listPolicies",
        "iam:listPolicyVersions",
        "iam:listRolePolicies",
        "iam:listRoles",
        "iam:listSAMLProviders",
        "iam:listSSHPublicKeys",
        "iam:listServerCertificates",
        "iam:listSigningCertificates",
        "iam:listUserPolicies",
        "iam:listUsers",
        "iam:listVirtualMFADevices",
        "kafka:describeCluster",
        "kafka:describeClusterOperation",
        "kafka:describeClusterOperationV2",
        "kafka:describeClusterV2",
        "kafka:describeConfiguration",
        "kafka:describeConfigurationRevision",
        "kafka:describeReplicator",
        "kafka:describeVpcConnection",
        "kafka:getBootstrapBrokers",
        "kafka:getClusterPolicy",
        "kafka:listClientVpcConnections",
        "kafka:listClusterOperations",
        "kafka:listClusterOperationsV2",
        "kafka:listClusters",
        "kafka:listClustersV2",
        "kafka:listConfigurationRevisions",
        "kafka:listConfigurations",
        "kafka:listNodes",
        "kafka:listReplicators",
        "kafka:listScramSecrets",
        "kafka:listVpcConnections",
        "kafkaconnect:describeConnector",
        "kafkaconnect:describeCustomPlugin",
        "kafkaconnect:describeWorkerConfiguration",
        "kafkaconnect:listConnectors",
        "kafkaconnect:listCustomPlugins",
```

```
        "kafkaconnect:listWorkerConfigurations",
        "lambda:getAccountSettings",
        "lambda:getAlias",
        "lambda:getCodeSigningConfig",
        "lambda:getEventSourceMapping",
        "lambda:getFunction",
        "lambda:getFunctionCodeSigningConfig",
        "lambda:getFunctionConcurrency",
        "lambda:getFunctionConfiguration",
        "lambda:getFunctionEventInvokeConfig",
        "lambda:getFunctionUrlConfig",
        "lambda:getLayerVersion",
        "lambda:getLayerVersionPolicy",
        "lambda:getPolicy",
        "lambda:getProvisionedConcurrencyConfig",
        "lambda:getRuntimeManagementConfig",
        "lambda:listAliases",
        "lambda:listCodeSigningConfigs",
        "lambda:listEventSourceMappings",
        "lambda:listFunctionEventInvokeConfigs",
        "lambda:listFunctionUrlConfigs",
        "lambda:listFunctions",
        "lambda:listFunctionsByCodeSigningConfig",
        "lambda:listLayerVersions",
        "lambda:listLayers",
        "lambda:listProvisionedConcurrencyConfigs",
        "lambda:listVersionsByFunction",
        "logs:describeExportTasks",
        "logs:describeLogGroups",
        "logs:describeLogStreams",
        "logs:describeMetricFilters",
        "logs:describeSubscriptionFilters",
        "medialive:listChannels",
        "medialive:listInputSecurityGroups",
        "medialive:listInputs",
        "mobiletargeting:getAdmChannel",
        "mobiletargeting:getApnsChannel",
        "mobiletargeting:getApnsSandboxChannel",
        "mobiletargeting:getApnsVoipChannel",
        "mobiletargeting:getApnsVoipSandboxChannel",
        "mobiletargeting:getApplicationSettings",
        "mobiletargeting:getApps",
        "mobiletargeting:getBaiduChannel",
        "mobiletargeting:getCampaign",
```

```
        "mobiletargeting:getCampaignActivities",
        "mobiletargeting:getCampaignVersions",
        "mobiletargeting:getCampaigns",
        "mobiletargeting:getEmailChannel",
        "mobiletargeting:getEventStream",
        "mobiletargeting:getExportJobs",
        "mobiletargeting:getGcmChannel",
        "mobiletargeting:getImportJobs",
        "mobiletargeting:getJourney",
        "mobiletargeting:getJourneyExecutionActivityMetrics",
        "mobiletargeting:getJourneyExecutionMetrics",
        "mobiletargeting:getJourneyRunExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionMetrics",
        "mobiletargeting:getJourneyRuns",
        "mobiletargeting:getSegment",
        "mobiletargeting:getSegmentImportJobs",
        "mobiletargeting:getSegmentVersions",
        "mobiletargeting:getSegments",
        "mobiletargeting:getSmsChannel",
        "mobiletargeting:listJourneys",
        "pipes:listPipes",
        "polly:describeVoices",
        "polly:listLexicons",
        "quicksight:describeAccountCustomization",
        "quicksight:describeAccountSettings",
        "quicksight:describeAccountSubscription",
        "quicksight:describeAnalysis",
        "quicksight:describeAnalysisPermissions",
        "quicksight:describeDashboard",
        "quicksight:describeDashboardPermissions",
        "quicksight:describeDataSet",
        "quicksight:describeDataSetRefreshProperties",
        "quicksight:describeDataSource",
        "quicksight:describeFolder",
        "quicksight:describeFolderPermissions",
        "quicksight:describeFolderResolvedPermissions",
        "quicksight:describeGroup",
        "quicksight:describeGroupMembership",
        "quicksight:describeIAMPolicyAssignment",
        "quicksight:describeIngestion",
        "quicksight:describeIpRestriction",
        "quicksight:describeNamespace",
        "quicksight:describeRefreshSchedule",
        "quicksight:describeTemplate",
```

```
        "quicksight:describeTemplateAlias",
        "quicksight:describeTemplatePermissions",
        "quicksight:describeTheme",
        "quicksight:describeThemeAlias",
        "quicksight:describeThemePermissions",
        "quicksight:describeTopic",
        "quicksight:describeTopicRefresh",
        "quicksight:describeTopicRefreshSchedule",
        "quicksight:describeUser",
        "quicksight:describeVPCConnection",
        "quicksight:listAnalyses",
        "quicksight:listDashboardVersions",
        "quicksight:listDashboards",
        "quicksight:listDataSets",
        "quicksight:listDataSources",
        "quicksight:listFolderMembers",
        "quicksight:listFolders",
        "quicksight:listGroupMemberships",
        "quicksight:listGroups",
        "quicksight:listIAMPolicyAssignments",
        "quicksight:listIAMPolicyAssignmentsForUser",
        "quicksight:listIngestions",
        "quicksight:listNamespaces",
        "quicksight:listRefreshSchedules",
        "quicksight:listTemplateAliases",
        "quicksight:listTemplateVersions",
        "quicksight:listTemplates",
        "quicksight:listThemeAliases",
        "quicksight:listThemeVersions",
        "quicksight:listThemes",
        "quicksight:listTopicRefreshSchedules",
        "quicksight:listTopics",
        "quicksight:listUserGroups",
        "quicksight:listUsers",
        "quicksight:listVPCConnections",
        "quicksight:searchAnalyses",
        "quicksight:searchDashboards",
        "quicksight:searchDataSets",
        "quicksight:searchDataSources",
        "quicksight:searchFolders",
        "quicksight:searchGroups",
        "rds:describeAccountAttributes",
        "rds:describeBlueGreenDeployments",
        "rds:describeCertificates",
```

```
        "rds:describeDBClusterEndpoints",
        "rds:describeDBClusterParameterGroups",
        "rds:describeDBClusterParameters",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusters",
        "rds:describeDBEngineVersions",
        "rds:describeDBInstanceAutomatedBackups",
        "rds:describeDBInstances",
        "rds:describeDBLogFiles",
        "rds:describeDBParameterGroups",
        "rds:describeDBParameters",
        "rds:describeDBSecurityGroups",
        "rds:describeDBSnapshotAttributes",
        "rds:describeDBSnapshots",
        "rds:describeDBSubnetGroups",
        "rds:describeEngineDefaultClusterParameters",
        "rds:describeEngineDefaultParameters",
        "rds:describeEventCategories",
        "rds:describeEventSubscriptions",
        "rds:describeEvents",
        "rds:describeExportTasks",
        "rds:describeGlobalClusters",
        "rds:describeIntegrations",
        "rds:describeOptionGroupOptions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describePendingMaintenanceActions",
        "rds:describeReservedDBInstances",
        "rds:describeReservedDBInstancesOfferings",
        "rds:describeSourceRegions",
        "rds:describeValidDBInstanceModifications",
        "rds:listTagsForResource",
        "redshift-data:describeStatement",
        "redshift-data:listStatements",
        "redshift-serverless:getEndpointAccess",
        "redshift-serverless:getNamespace",
        "redshift-serverless:getRecoveryPoint",
        "redshift-serverless:getSnapshot",
        "redshift-serverless:getTableRestoreStatus",
        "redshift-serverless:getUsageLimit",
        "redshift-serverless:getWorkgroup",
        "redshift-serverless:listEndpointAccess",
        "redshift-serverless:listNamespaces",
        "redshift-serverless:listRecoveryPoints",
```

```
        "redshift-serverless:listSnapshots",
        "redshift-serverless:listTableRestoreStatus",
        "redshift-serverless:listUsageLimits",
        "redshift-serverless:listWorkgroups",
        "redshift:describeClusterParameterGroups",
        "redshift:describeClusterParameters",
        "redshift:describeClusterSecurityGroups",
        "redshift:describeClusterSnapshots",
        "redshift:describeClusterSubnetGroups",
        "redshift:describeClusterVersions",
        "redshift:describeClusters",
        "redshift:describeDataShares",
        "redshift:describeDataSharesForConsumer",
        "redshift:describeDataSharesForProducer",
        "redshift:describeDefaultClusterParameters",
        "redshift:describeEventCategories",
        "redshift:describeEventSubscriptions",
        "redshift:describeEvents",
        "redshift:describeHsmClientCertificates",
        "redshift:describeHsmConfigurations",
        "redshift:describeLoggingStatus",
        "redshift:describeOrderableClusterOptions",
        "redshift:describeReservedNodeOfferings",
        "redshift:describeReservedNodes",
        "redshift:describeResize",
        "redshift:describeSnapshotCopyGrants",
        "redshift:describeStorage",
        "redshift:describeTableRestoreStatus",
        "redshift:describeTags",
        "route53-recovery-cluster:getRoutingControlState",
        "route53-recovery-cluster:listRoutingControls",
        "route53-recovery-control-config:describeControlPanel",
        "route53-recovery-control-config:describeRoutingControl",
        "route53-recovery-control-config:describeSafetyRule",
        "route53-recovery-control-config:listControlPanels",
        "route53-recovery-control-config:listRoutingControls",
        "route53-recovery-control-config:listSafetyRules",
        "route53-recovery-readiness:getCell",
        "route53-recovery-readiness:getCellReadinessSummary",
        "route53-recovery-readiness:getReadinessCheck",
        "route53-recovery-readiness:getReadinessCheckResourceStatus",
        "route53-recovery-readiness:getReadinessCheckStatus",
        "route53-recovery-readiness:getRecoveryGroup",
        "route53-recovery-readiness:getRecoveryGroupReadinessSummary",
```

```
        "route53-recovery-readiness:listCells",
        "route53-recovery-readiness:listReadinessChecks",
        "route53-recovery-readiness:listRecoveryGroups",
        "route53-recovery-readiness:listResourceSets",
        "route53:getAccountLimit",
        "route53:getChange",
        "route53:getCheckerIpRanges",
        "route53:getDNSSEC",
        "route53:getGeoLocation",
        "route53:getHealthCheck",
        "route53:getHealthCheckCount",
        "route53:getHealthCheckLastFailureReason",
        "route53:getHealthCheckStatus",
        "route53:getHostedZone",
        "route53:getHostedZoneCount",
        "route53:getHostedZoneLimit",
        "route53:getQueryLoggingConfig",
        "route53:getReusableDelegationSet",
        "route53:getTrafficPolicy",
        "route53:getTrafficPolicyInstance",
        "route53:getTrafficPolicyInstanceCount",
        "route53:listCidrBlocks",
        "route53:listCidrCollections",
        "route53:listCidrLocations",
        "route53:listGeoLocations",
        "route53:listHealthChecks",
        "route53:listHostedZones",
        "route53:listHostedZonesByName",
        "route53:listHostedZonesByVpc",
        "route53:listQueryLoggingConfigs",
        "route53:listResourceRecordSets",
        "route53:listReusableDelegationSets",
        "route53:listTrafficPolicies",
        "route53:listTrafficPolicyInstances",
        "route53:listTrafficPolicyInstancesByHostedZone",
        "route53:listTrafficPolicyInstancesByPolicy",
        "route53:listTrafficPolicyVersions",
        "route53:listVPCAssociationAuthorizations",
        "route53domains:checkDomainAvailability",
        "route53domains:getContactReachabilityStatus",
        "route53domains:getDomainDetail",
        "route53domains:getOperationDetail",
        "route53domains:listDomains",
        "route53domains:listOperations",
```

```
        "route53domains:listPrices",
        "route53domains:listTagsForDomain",
        "route53domains:viewBilling",
        "route53resolver:getFirewallConfig",
        "route53resolver:getFirewallDomainList",
        "route53resolver:getFirewallRuleGroup",
        "route53resolver:getFirewallRuleGroupAssociation",
        "route53resolver:getFirewallRuleGroupPolicy",
        "route53resolver:getOutpostResolver",
        "route53resolver:getResolverDnssecConfig",
        "route53resolver:getResolverQueryLogConfig",
        "route53resolver:getResolverQueryLogConfigAssociation",
        "route53resolver:getResolverQueryLogConfigPolicy",
        "route53resolver:getResolverRule",
        "route53resolver:getResolverRuleAssociation",
        "route53resolver:getResolverRulePolicy",
        "route53resolver:listFirewallConfigs",
        "route53resolver:listFirewallDomainLists",
        "route53resolver:listFirewallDomains",
        "route53resolver:listFirewallRuleGroupAssociations",
        "route53resolver:listFirewallRuleGroups",
        "route53resolver:listFirewallRules",
        "route53resolver:listOutpostResolvers",
        "route53resolver:listResolverConfigs",
        "route53resolver:listResolverDnssecConfigs",
        "route53resolver:listResolverEndpointIpAddresses",
        "route53resolver:listResolverEndpoints",
        "route53resolver:listResolverQueryLogConfigAssociations",
        "route53resolver:listResolverQueryLogConfigs",
        "route53resolver:listResolverRuleAssociations",
        "route53resolver:listResolverRules",
        "route53resolver:listTagsForResource",
        "s3:describeJob",
        "s3:describeMultiRegionAccessPointOperation",
        "s3:getAccelerateConfiguration",
        "s3:getAccessPoint",
        "s3:getAccessPointConfigurationForObjectLambda",
        "s3:getAccessPointForObjectLambda",
        "s3:getAccessPointPolicy",
        "s3:getAccessPointPolicyForObjectLambda",
        "s3:getAccessPointPolicyStatus",
        "s3:getAccessPointPolicyStatusForObjectLambda",
        "s3:getAccountPublicAccessBlock",
        "s3:getAnalyticsConfiguration",
```

```
            "s3:getBucketAcl",
            "s3:getBucketCORS",
            "s3:getBucketLocation",
            "s3:getBucketLogging",
            "s3:getBucketNotification",
            "s3:getBucketObjectLockConfiguration",
            "s3:getBucketOwnershipControls",
            "s3:getBucketPolicy",
            "s3:getBucketPolicyStatus",
            "s3:getBucketPublicAccessBlock",
            "s3:getBucketRequestPayment",
            "s3:getBucketVersioning",
            "s3:getBucketWebsite",
            "s3:getEncryptionConfiguration",
            "s3:getIntelligentTieringConfiguration",
            "s3:getInventoryConfiguration",
            "s3:getLifecycleConfiguration",
            "s3:getMetricsConfiguration",
            "s3:getMultiRegionAccessPoint",
            "s3:getMultiRegionAccessPointPolicy",
            "s3:getMultiRegionAccessPointPolicyStatus",
            "s3:getMultiRegionAccessPointRoutes",
            "s3:getObjectLegalHold",
            "s3:getObjectRetention",
            "s3:getReplicationConfiguration",
            "s3:getStorageLensConfiguration",
            "s3:listAccessPoints",
            "s3:listAccessPointsForObjectLambda",
            "s3:listAllMyBuckets",
            "s3:listBucket",
            "s3:listBucketMultipartUploads",
            "s3:listBucketVersions",
            "s3:listJobs",
            "s3:listMultiRegionAccessPoints",
            "s3:listMultipartUploadParts",
            "s3:listStorageLensConfigurations",
            "s3express:getBucketPolicy",
            "s3express:listAllMyDirectoryBuckets",
            "sagemaker:describeAction",
            "sagemaker:describeAlgorithm",
            "sagemaker:describeApp",
            "sagemaker:describeAppImageConfig",
            "sagemaker:describeArtifact",
            "sagemaker:describeAutoMLJob",
```

```
            "sagemaker:describeCluster",
            "sagemaker:describeClusterNode",
            "sagemaker:describeCodeRepository",
            "sagemaker:describeCompilationJob",
            "sagemaker:describeContext",
            "sagemaker:describeDataQualityJobDefinition",
            "sagemaker:describeDevice",
            "sagemaker:describeDeviceFleet",
            "sagemaker:describeDomain",
            "sagemaker:describeEdgeDeploymentPlan",
            "sagemaker:describeEdgePackagingJob",
            "sagemaker:describeEndpoint",
            "sagemaker:describeEndpointConfig",
            "sagemaker:describeExperiment",
            "sagemaker:describeFeatureGroup",
            "sagemaker:describeFeatureMetadata",
            "sagemaker:describeFlowDefinition",
            "sagemaker:describeHub",
            "sagemaker:describeHubContent",
            "sagemaker:describeHumanTaskUi",
            "sagemaker:describeHyperParameterTuningJob",
            "sagemaker:describeImage",
            "sagemaker:describeImageVersion",
            "sagemaker:describeInferenceComponent",
            "sagemaker:describeInferenceExperiment",
            "sagemaker:describeInferenceRecommendationsJob",
            "sagemaker:describeLabelingJob",
            "sagemaker:describeModel",
            "sagemaker:describeModelBiasJobDefinition",
            "sagemaker:describeModelCard",
            "sagemaker:describeModelCardExportJob",
            "sagemaker:describeModelExplainabilityJobDefinition",
            "sagemaker:describeModelPackage",
            "sagemaker:describeModelPackageGroup",
            "sagemaker:describeModelQualityJobDefinition",
            "sagemaker:describeMonitoringSchedule",
            "sagemaker:describeNotebookInstance",
            "sagemaker:describeNotebookInstanceLifecycleConfig",
            "sagemaker:describePipeline",
            "sagemaker:describePipelineDefinitionForExecution",
            "sagemaker:describePipelineExecution",
            "sagemaker:describeProcessingJob",
            "sagemaker:describeProject",
            "sagemaker:describeSpace",
```

```
        "sagemaker:describeStudioLifecycleConfig",
        "sagemaker:describeSubscribedWorkteam",
        "sagemaker:describeTrainingJob",
        "sagemaker:describeTransformJob",
        "sagemaker:describeTrial",
        "sagemaker:describeTrialComponent",
        "sagemaker:describeUserProfile",
        "sagemaker:describeWorkforce",
        "sagemaker:describeWorkteam",
        "sagemaker:getDeviceFleetReport",
        "sagemaker:getModelPackageGroupPolicy",
        "sagemaker:getSagemakerServicecatalogPortfolioStatus",
        "sagemaker:listActions",
        "sagemaker:listAlgorithms",
        "sagemaker:listAliases",
        "sagemaker:listAppImageConfigs",
        "sagemaker:listApps",
        "sagemaker:listArtifacts",
        "sagemaker:listAssociations",
        "sagemaker:listAutoMLJobs",
        "sagemaker:listCandidatesForAutoMLJob",
        "sagemaker:listClusterNodes",
        "sagemaker:listClusters",
        "sagemaker:listCodeRepositories",
        "sagemaker:listCompilationJobs",
        "sagemaker:listContexts",
        "sagemaker:listDataQualityJobDefinitions",
        "sagemaker:listDeviceFleets",
        "sagemaker:listDevices",
        "sagemaker:listDomains",
        "sagemaker:listEdgeDeploymentPlans",
        "sagemaker:listEdgePackagingJobs",
        "sagemaker:listEndpointConfigs",
        "sagemaker:listEndpoints",
        "sagemaker:listExperiments",
        "sagemaker:listFeatureGroups",
        "sagemaker:listFlowDefinitions",
        "sagemaker:listHubContentVersions",
        "sagemaker:listHubContents",
        "sagemaker:listHubs",
        "sagemaker:listHumanTaskUis",
        "sagemaker:listHyperParameterTuningJobs",
        "sagemaker:listImageVersions",
        "sagemaker:listImages",
```

```
        "sagemaker:listInferenceComponents",
        "sagemaker:listInferenceExperiments",
        "sagemaker:listInferenceRecommendationsJobSteps",
        "sagemaker:listInferenceRecommendationsJobs",
        "sagemaker:listLabelingJobs",
        "sagemaker:listLabelingJobsForWorkteam",
        "sagemaker:listLineageGroups",
        "sagemaker:listModelBiasJobDefinitions",
        "sagemaker:listModelCardExportJobs",
        "sagemaker:listModelCardVersions",
        "sagemaker:listModelCards",
        "sagemaker:listModelExplainabilityJobDefinitions",
        "sagemaker:listModelMetadata",
        "sagemaker:listModelPackageGroups",
        "sagemaker:listModelPackages",
        "sagemaker:listModelQualityJobDefinitions",
        "sagemaker:listModels",
        "sagemaker:listMonitoringAlertHistory",
        "sagemaker:listMonitoringAlerts",
        "sagemaker:listMonitoringExecutions",
        "sagemaker:listMonitoringSchedules",
        "sagemaker:listNotebookInstanceLifecycleConfigs",
        "sagemaker:listNotebookInstances",
        "sagemaker:listPipelineExecutionSteps",
        "sagemaker:listPipelineExecutions",
        "sagemaker:listPipelineParametersForExecution",
        "sagemaker:listPipelines",
        "sagemaker:listProcessingJobs",
        "sagemaker:listProjects",
        "sagemaker:listSpaces",
        "sagemaker:listStageDevices",
        "sagemaker:listStudioLifecycleConfigs",
        "sagemaker:listSubscribedWorkteams",
        "sagemaker:listTags",
        "sagemaker:listTrainingJobs",
        "sagemaker:listTrainingJobsForHyperParameterTuningJob",
        "sagemaker:listTransformJobs",
        "sagemaker:listTrialComponents",
        "sagemaker:listTrials",
        "sagemaker:listUserProfiles",
        "sagemaker:listWorkforces",
        "sagemaker:listWorkteams",
        "scheduler:listScheduleGroups",
        "scheduler:listSchedules",
```

```
        "servicequotas:listAWSDefaultServiceQuotas",
        "servicequotas:listServiceQuotas",
        "ses:describeActiveReceiptRuleSet",
        "ses:describeConfigurationSet",
        "ses:describeReceiptRule",
        "ses:describeReceiptRuleSet",
        "ses:getAccount",
        "ses:getAccountSendingEnabled",
        "ses:getBlacklistReports",
        "ses:getConfigurationSet",
        "ses:getConfigurationSetEventDestinations",
        "ses:getContactList",
        "ses:getDedicatedIp",
        "ses:getDedicatedIpPool",
        "ses:getDedicatedIps",
        "ses:getDeliverabilityDashboardOptions",
        "ses:getDeliverabilityTestReport",
        "ses:getDomainDeliverabilityCampaign",
        "ses:getDomainStatisticsReport",
        "ses:getEmailIdentity",
        "ses:getIdentityDkimAttributes",
        "ses:getIdentityMailFromDomainAttributes",
        "ses:getIdentityNotificationAttributes",
        "ses:getIdentityPolicies",
        "ses:getIdentityVerificationAttributes",
        "ses:getImportJob",
        "ses:getSendQuota",
        "ses:getSendStatistics",
        "ses:listConfigurationSets",
        "ses:listContactLists",
        "ses:listContacts",
        "ses:listCustomVerificationEmailTemplates",
        "ses:listDedicatedIpPools",
        "ses:listDeliverabilityTestReports",
        "ses:listDomainDeliverabilityCampaigns",
        "ses:listEmailIdentities",
        "ses:listEmailTemplates",
        "ses:listIdentities",
        "ses:listIdentityPolicies",
        "ses:listImportJobs",
        "ses:listReceiptFilters",
        "ses:listReceiptRuleSets",
        "ses:listRecommendations",
        "ses:listTagsForResource",
```

```
        "ses:listTemplates",
        "ses:listVerifiedEmailAddresses",
        "sns:checkIfPhoneNumberIsOptedOut",
        "sns:getDataProtectionPolicy",
        "sns:getEndpointAttributes",
        "sns:getPlatformApplicationAttributes",
        "sns:getSMSAttributes",
        "sns:getSMSSandboxAccountStatus",
        "sns:getSubscriptionAttributes",
        "sns:getTopicAttributes",
        "sns:listEndpointsByPlatformApplication",
        "sns:listOriginationNumbers",
        "sns:listPhoneNumbersOptedOut",
        "sns:listPlatformApplications",
        "sns:listSMSSandboxPhoneNumbers",
        "sns:listSubscriptions",
        "sns:listSubscriptionsByTopic",
        "sns:listTopics",
        "ssm-contacts:describeEngagement",
        "ssm-contacts:describePage",
        "ssm-contacts:getContact",
        "ssm-contacts:getContactChannel",
        "ssm-contacts:getContactPolicy",
        "ssm-contacts:getRotation",
        "ssm-contacts:getRotationOverride",
        "ssm-contacts:listContactChannels",
        "ssm-contacts:listContacts",
        "ssm-contacts:listEngagements",
        "ssm-contacts:listPageReceipts",
        "ssm-contacts:listPageResolutions",
        "ssm-contacts:listPagesByContact",
        "ssm-contacts:listPagesByEngagement",
        "ssm-contacts:listPreviewRotationShifts",
        "ssm-contacts:listRotationOverrides",
        "ssm-contacts:listRotationShifts",
        "ssm-contacts:listRotations",
        "ssm-incidents:getIncidentRecord",
        "ssm-incidents:getReplicationSet",
        "ssm-incidents:getResourcePolicies",
        "ssm-incidents:getResponsePlan",
        "ssm-incidents:getTimelineEvent",
        "ssm-incidents:listIncidentRecords",
        "ssm-incidents:listRelatedItems",
        "ssm-incidents:listReplicationSets",
```

```
        "ssm-incidents:listResponsePlans",
        "ssm-incidents:listTimelineEvents",
        "ssm-sap:getApplication",
        "ssm-sap:getComponent",
        "ssm-sap:getDatabase",
        "ssm-sap:getOperation",
        "ssm-sap:getResourcePermission",
        "ssm-sap:listApplications",
        "ssm-sap:listComponents",
        "ssm-sap:listDatabases",
        "ssm-sap:listOperations",
        "ssm:describeActivations",
        "ssm:describeAssociation",
        "ssm:describeAssociationExecutionTargets",
        "ssm:describeAssociationExecutions",
        "ssm:describeAutomationExecutions",
        "ssm:describeAutomationStepExecutions",
        "ssm:describeAvailablePatches",
        "ssm:describeDocument",
        "ssm:describeDocumentPermission",
        "ssm:describeEffectiveInstanceAssociations",
        "ssm:describeEffectivePatchesForPatchBaseline",
        "ssm:describeInstanceAssociationsStatus",
        "ssm:describeInstanceInformation",
        "ssm:describeInstancePatchStates",
        "ssm:describeInstancePatchStatesForPatchGroup",
        "ssm:describeInstancePatches",
        "ssm:describeInventoryDeletions",
        "ssm:describeMaintenanceWindowExecutionTaskInvocations",
        "ssm:describeMaintenanceWindowExecutionTasks",
        "ssm:describeMaintenanceWindowExecutions",
        "ssm:describeMaintenanceWindowSchedule",
        "ssm:describeMaintenanceWindowTargets",
        "ssm:describeMaintenanceWindowTasks",
        "ssm:describeMaintenanceWindows",
        "ssm:describeMaintenanceWindowsForTarget",
        "ssm:describeOpsItems",
        "ssm:describeParameters",
        "ssm:describePatchBaselines",
        "ssm:describePatchGroupState",
        "ssm:describePatchGroups",
        "ssm:describePatchProperties",
        "ssm:describeSessions",
        "ssm:getAutomationExecution",
```

```
        "ssm:getCalendarState",
        "ssm:getCommandInvocation",
        "ssm:getConnectionStatus",
        "ssm:getDefaultPatchBaseline",
        "ssm:getDeployablePatchSnapshotForInstance",
        "ssm:getInventorySchema",
        "ssm:getMaintenanceWindow",
        "ssm:getMaintenanceWindowExecution",
        "ssm:getMaintenanceWindowExecutionTask",
        "ssm:getMaintenanceWindowExecutionTaskInvocation",
        "ssm:getMaintenanceWindowTask",
        "ssm:getOpsItem",
        "ssm:getOpsMetadata",
        "ssm:getOpsSummary",
        "ssm:getPatchBaseline",
        "ssm:getPatchBaselineForPatchGroup",
        "ssm:getResourcePolicies",
        "ssm:getServiceSetting",
        "ssm:listAssociationVersions",
        "ssm:listAssociations",
        "ssm:listCommandInvocations",
        "ssm:listCommands",
        "ssm:listComplianceItems",
        "ssm:listComplianceSummaries",
        "ssm:listDocumentMetadataHistory",
        "ssm:listDocumentVersions",
        "ssm:listDocuments",
        "ssm:listOpsItemEvents",
        "ssm:listOpsItemRelatedItems",
        "ssm:listOpsMetadata",
        "ssm:listResourceComplianceSummaries",
        "ssm:listResourceDataSync",
        "ssm:listTagsForResource",
        "swf:describeActivityType",
        "swf:describeDomain",
        "swf:describeWorkflowExecution",
        "swf:describeWorkflowType",
        "swf:getWorkflowExecutionHistory",
        "swf:listActivityTypes",
        "swf:listClosedWorkflowExecutions",
        "swf:listDomains",
        "swf:listOpenWorkflowExecutions",
        "swf:listWorkflowTypes",
        "vpc-lattice:getAccessLogSubscription",
```

```
        "vpc-lattice:getAuthPolicy",
        "vpc-lattice:getListener",
        "vpc-lattice:getResourcePolicy",
        "vpc-lattice:getRule",
        "vpc-lattice:getService",
        "vpc-lattice:getServiceNetwork",
        "vpc-lattice:getServiceNetworkServiceAssociation",
        "vpc-lattice:getServiceNetworkVpcAssociation",
        "vpc-lattice:getTargetGroup",
        "vpc-lattice:listAccessLogSubscriptions",
        "vpc-lattice:listListeners",
        "vpc-lattice:listRules",
        "vpc-lattice:listServiceNetworkServiceAssociations",
        "vpc-lattice:listServiceNetworkVpcAssociations",
        "vpc-lattice:listServiceNetworks",
        "vpc-lattice:listServices",
        "vpc-lattice:listTargetGroups",
        "vpc-lattice:listTargets",
        "waf-regional:getByteMatchSet",
        "waf-regional:getChangeTokenStatus",
        "waf-regional:getGeoMatchSet",
        "waf-regional:getIPSet",
        "waf-regional:getLoggingConfiguration",
        "waf-regional:getRateBasedRule",
        "waf-regional:getRegexMatchSet",
        "waf-regional:getRegexPatternSet",
        "waf-regional:getRule",
        "waf-regional:getRuleGroup",
        "waf-regional:getSqlInjectionMatchSet",
        "waf-regional:getWebACL",
        "waf-regional:getWebACLForResource",
        "waf-regional:listActivatedRulesInRuleGroup",
        "waf-regional:listByteMatchSets",
        "waf-regional:listGeoMatchSets",
        "waf-regional:listIPSets",
        "waf-regional:listLoggingConfigurations",
        "waf-regional:listRateBasedRules",
        "waf-regional:listRegexMatchSets",
        "waf-regional:listRegexPatternSets",
        "waf-regional:listResourcesForWebACL",
        "waf-regional:listRuleGroups",
        "waf-regional:listRules",
        "waf-regional:listSqlInjectionMatchSets",
        "waf-regional:listWebACLs",
```

```
        "waf:getByteMatchSet",
        "waf:getChangeTokenStatus",
        "waf:getGeoMatchSet",
        "waf:getIPSet",
        "waf:getLoggingConfiguration",
        "waf:getRateBasedRule",
        "waf:getRegexMatchSet",
        "waf:getRegexPatternSet",
        "waf:getRule",
        "waf:getRuleGroup",
        "waf:getSampledRequests",
        "waf:getSizeConstraintSet",
        "waf:getSqlInjectionMatchSet",
        "waf:getWebACL",
        "waf:getXssMatchSet",
        "waf:listActivatedRulesInRuleGroup",
        "waf:listByteMatchSets",
        "waf:listGeoMatchSets",
        "waf:listIPSets",
        "waf:listLoggingConfigurations",
        "waf:listRateBasedRules",
        "waf:listRegexMatchSets",
        "waf:listRegexPatternSets",
        "waf:listRuleGroups",
        "waf:listRules",
        "waf:listSizeConstraintSets",
        "waf:listSqlInjectionMatchSets",
        "waf:listWebACLs",
        "waf:listXssMatchSets",
        "wafv2:checkCapacity",
        "wafv2:describeManagedRuleGroup",
        "wafv2:getIPSet",
        "wafv2:getLoggingConfiguration",
        "wafv2:getPermissionPolicy",
        "wafv2:getRateBasedStatementManagedKeys",
        "wafv2:getRegexPatternSet",
        "wafv2:getRuleGroup",
        "wafv2:getSampledRequests",
        "wafv2:getWebACL",
        "wafv2:getWebACLForResource",
        "wafv2:listAvailableManagedRuleGroups",
        "wafv2:listIPSets",
        "wafv2:listLoggingConfigurations",
        "wafv2:listRegexPatternSets",
```

```
        "wafv2:listResourcesForWebACL",
        "wafv2:listRuleGroups",
        "wafv2:listTagsForResource",
        "wafv2:listWebACLs",
        "workspaces-web:getBrowserSettings",
        "workspaces-web:getIdentityProvider",
        "workspaces-web:getNetworkSettings",
        "workspaces-web:getPortal",
        "workspaces-web:getPortalServiceProviderMetadata",
        "workspaces-web:getTrustStoreCertificate",
        "workspaces-web:getUserSettings",
        "workspaces-web:listBrowserSettings",
        "workspaces-web:listIdentityProviders",
        "workspaces-web:listNetworkSettings",
        "workspaces-web:listPortals",
        "workspaces-web:listTagsForResource",
        "workspaces-web:listTrustStoreCertificates",
        "workspaces-web:listTrustStores",
        "workspaces-web:listUserSettings",
        "workspaces:describeAccount",
        "workspaces:describeAccountModifications",
        "workspaces:describeApplicationAssociations",
        "workspaces:describeIpGroups",
        "workspaces:describeTags",
        "workspaces:describeWorkspaceAssociations",
        "workspaces:describeWorkspaceBundles",
        "workspaces:describeWorkspaceDirectories",
        "workspaces:describeWorkspaceImages",
        "workspaces:describeWorkspaces",
        "workspaces:describeWorkspacesConnectionStatus"
      ],
      "Resource" : [
        "*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPartnerProServeToolsFullAccess

Descrição: Fornece acesso total às ProServe ferramentas.

`AWSPartnerProServeToolsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPartnerProServeToolsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 23 de março de 2026, 21:57 UTC
- Horário editado: 23 de março de 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerProServeToolsFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowProServeToolsFullAccess",
```

```
      "Effect" : "Allow",
      "Action" : "partnercentral-account-management:AccessProServeTools",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "partnercentral-account-management:ProServeRole" : [
            "AssessmentIndividualContributor",
            "AssessmentOrganizationReader",
            "AssessmentOrganizationContributor",
            "OrganizationAdmin"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPartnerProServeToolsIndividualContributor

Descrição: Fornece acesso para criar e gerenciar suas próprias avaliações em ProServe ferramentas.

`AWSPartnerProServeToolsIndividualContributor` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPartnerProServeToolsIndividualContributor` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Horário de criação: 23 de março de 2026, 21:57 UTC
- Horário editado: 23 de março de 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerProServeToolsIndividualContributor`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowProServeToolsIndividualContributorAccess",
      "Effect" : "Allow",
      "Action" : "partnercentral-account-management:AccessProServeTools",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "partnercentral-account-management:ProServeRole" : [
            "AssessmentIndividualContributor"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPartnerProServeToolsOrganizationReaderIndividualContributor

Descrição: Fornece acesso de leitura às avaliações organizacionais com a capacidade de gerenciar suas próprias avaliações.

`AWSPartnerProServeToolsOrganizationReaderIndividualContributor` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPartnerProServeToolsOrganizationReaderIndividualContributor` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 23 de março de 2026, 22:12 UTC
- Horário editado: 23 de março de 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerProServeToolsOrganizationReaderIndividualContributor`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowProServeToolsOrgReaderIndividualContributorAccess",
```

```
      "Effect" : "Allow",
      "Action" : "partnercentral-account-management:AccessProServeTools",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "partnercentral-account-management:ProServeRole" : [
            "AssessmentOrganizationReader",
            "AssessmentIndividualContributor"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPCSComputeNodePolicy

Descrição: Concede permissão aos nós de computação do AWS PCS para se conectarem aos clusters do AWS PCS.

`AWSPCSComputeNodePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPCSComputeNodePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 23 de junho de 2025, 18:07 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC

- ARN: `arn:aws:iam::aws:policy/AWSPCSComputeNodePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pcs:RegisterComputeNodeGroupInstance"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPCSServiceRolePolicy

Descrição: concede permissões ao PCS para gerenciar recursos em seu nome.

`AWSPCSServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 27 de agosto de 2024, 16:01 UTC
- Horário editado: 30 de setembro de 2026, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPCSServiceRolePolicy`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsToCreatePCSNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "PermissionsToCreatePCSNetworkInterfacesInSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "PermissionsToManagePCSNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToDescribePCSResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeTags"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsToCreatePCSLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToManagePCSLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTerminatePCSManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "PermissionsToPassRoleToEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*/AWSPCS*",
        "arn:aws:iam::*:role/AWSPCS*",
        "arn:aws:iam::*:role/aws-pcs/*",
        "arn:aws:iam::*:role/*/aws-pcs/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToControlClusterInstanceAttributes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:resource-groups:*:*:group/*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:spot-instances-request/*",
        "arn:aws:ec2:*:*:secondary-interface/*",
        "arn:aws:ec2:*:*:secondary-subnet/*"
      ]
    },
    {
      "Sid" : "PermissionsToProvisionClusterInstances",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTagPCSResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateLaunchTemplate",
            "CreateFleet",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToPublishMetrics",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/PCS"
        }
      }
```

```
    },
    {
      "Sid" : "PermissionsToManageSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:pcs!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "pcs",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPriceListServiceFullAccess

Descrição: Fornece acesso total ao Serviço de Lista de AWS Preços.

`AWSPriceListServiceFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPriceListServiceFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 22 de novembro de 2017, 0:36 UTC

- Hora da edição: 2 de julho de 2024, 13:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSPriceListServiceFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pricing:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPrivateCAAuditor

Descrição: Fornece acesso do auditor à Autoridade AWS Certificadora Privada

`AWSPrivateCAAuditor` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPrivateCAAuditor` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de fevereiro de 2023, 18:33 UTC
- Hora da edição: 14 de fevereiro de 2023, 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAAuditor`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:CreateCertificateAuthorityAuditReport",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:GetPolicy",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags"
      ],
```

```
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPrivateCAConnectorForKubernetesPolicy

Descrição: concede permissões essenciais para o AWS Private CA Connector for Kubernetes.

`AWSPrivateCAConnectorForKubernetesPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPrivateCAConnectorForKubernetesPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 19 de maio de 2025, 19:22 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAConnectorForKubernetesPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificate",
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPrivateCAFullAccess

Descrição: Fornece acesso total à Autoridade Certificadora AWS Privada

`AWSPrivateCAFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPrivateCAFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de fevereiro de 2023, 18:20 UTC
- Hora da edição: 14 de fevereiro de 2023, 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPrivateCAPrivilegedUser

Descrição: Fornece acesso privilegiado do usuário certificado à Autoridade Certificadora AWS Privada

`AWSPrivateCAPrivilegedUser` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPrivateCAPrivilegedUser` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de fevereiro de 2023, 18:26 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
```

```
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPrivateCAReadOnly

Descrição: Fornece acesso somente para leitura à Autoridade Certificadora AWS Privada

`AWSPrivateCAReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPrivateCAReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de fevereiro de 2023, 18:30 UTC
- Hora da edição: 14 de fevereiro de 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAReadOnly`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
```

```
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:ListCertificateAuthorities",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:GetPolicy",
      "acm-pca:ListPermissions",
      "acm-pca:ListTags"
    ],
    "Resource" : "*"
  }
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPrivateCAUser

Descrição: Fornece acesso do usuário certificado à Autoridade Certificadora AWS Privada

`AWSPrivateCAUser` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPrivateCAUser` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de fevereiro de 2023, 18:16 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAUser`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPrivateMarketplaceAdminFullAccess

Descrição: Fornece acesso total a todas as ações administrativas de um mercado AWS privado.

`AWSPrivateMarketplaceAdminFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPrivateMarketplaceAdminFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de novembro de 2018, 16:32 UTC

- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceGetRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*AWSServiceRoleForPrivateMarketplaceAdmin"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/private-
marketplace.marketplace.amazonaws.com/AWSServiceRoleForPrivateMarketplaceAdmin"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "private-marketplace.marketplace.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "PrivateMarketplaceManageDelegatedAdministratorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "private-
marketplace.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceEnableServiceAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "private-
marketplace.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceRequestPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:AssociateProductsWithPrivateMarketplace",
        "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCatalogAPIPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceCatalogTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "PrivateMarketplaceOrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPrivateMarketplaceRequests

Descrição: Fornece acesso à criação de solicitações em um mercado AWS privado.

`AWSPrivateMarketplaceRequests` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPrivateMarketplaceRequests` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário da criação: 28 de outubro de 2019, 21:44 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "LegacyPrivateMarketplaceRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceManageRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
            "CreateProductProcurementRequest",
            "CancelProductProcurementRequest"
          ]
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceReadRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceListRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:ListChangeSets"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceReadChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceTaggingRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPrivateNetworksServiceRolePolicy

Descrição: Permite que o AWS Private Networks Service gerencie recursos em nome do cliente.

`AWSPrivateNetworksServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 16 de dezembro de 2021, 23:17 UTC
- Hora da edição: 16 de dezembro de 2021, 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
```

```
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSProtonCodeBuildProvisioningBasicAccess

Descrição: As permissões CodeBuild precisam executar uma compilação para o CodeBuild provisionamento de AWS prótons.

`AWSProtonCodeBuildProvisioningBasicAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSProtonCodeBuildProvisioningBasicAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de novembro de 2022, 21:04 UTC
- Hora da edição: 09 de novembro de 2022, 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/AWSProton-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "proton:NotifyResourceDeploymentStatusChange",
      "Resource" : "arn:aws:proton:*:*:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSProtonCodeBuildProvisioningServiceRolePolicy

Descrição: permite que o AWS Proton gerencie o provisionamento de recursos do Proton usando CodeBuild e outros AWS serviços em seu nome.

`AWSProtonCodeBuildProvisioningServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 09 de novembro de 2022, 21:32 UTC
- Hora da edição: 17 de maio de 2023, 16:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ListStackResources"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSProton-CodeBuild-*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:UpdateProject",
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:RetryBuild",
        "codebuild:BatchGetBuilds",
        "codebuild:BatchGetProjects"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/AWSProton*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "codebuild.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSProtonDeveloperAccess

Descrição: Fornece acesso às APIs e ao console de gerenciamento do AWS Proton, mas não permite a administração de modelos ou ambientes do Proton.

`AWSProtonDeveloperAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSProtonDeveloperAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de fevereiro de 2021, 19:02 UTC
- Hora da edição: 6 de junho de 2024, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonDeveloperAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codestar-connections:ListConnections",
        "codestar-connections:UseConnection",
        "proton:CancelServiceInstanceDeployment",
        "proton:CancelServicePipelineDeployment",
```

```
        "proton:CreateService",
        "proton:DeleteService",
        "proton:GetAccountRoles",
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListRepositories",
        "proton:ListRepositorySyncDefinitions",
        "proton:ListServiceInstanceOutputs",
        "proton:ListServiceInstanceProvisionedResources",
        "proton:ListServiceInstances",
        "proton:ListServicePipelineOutputs",
        "proton:ListServicePipelineProvisionedResources",
        "proton:ListServices",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
        "proton:ListServiceTemplates",
        "proton:ListServiceTemplateVersions",
        "proton:ListTagsForResource",
        "proton:UpdateService",
        "proton:UpdateServiceInstance",
```

```
        "proton:UpdateServicePipeline",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "proton.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : "codeconnections:PassConnection",
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSProtonFullAccess

Descrição: Fornece acesso total às APIs do AWS Proton e ao console de gerenciamento. Além dessas permissões, o acesso ao Amazon S3 também é necessário para registrar pacotes de modelos de seus buckets do S3, bem como o acesso ao Amazon IAM para criar e gerenciar as funções de serviço do Proton.

`AWSProtonFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSProtonFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de fevereiro de 2021, 19:07 UTC
- Hora da edição: 6 de junho de 2024, 18:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "proton:*",
        "codestar-connections:ListConnections",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "proton.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "proton.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sync.proton.amazonaws.com/
AWSServiceRoleForProtonSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "sync.proton.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "CodeStarConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:PassConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "proton.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:PassConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSProtonReadOnlyAccess

Descrição: fornece acesso somente para leitura às APIs do AWS Proton e ao console de gerenciamento.

`AWSProtonReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSProtonReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de fevereiro de 2021, 19:09 UTC
- Hora da edição: 18 de novembro de 2022, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "proton:GetAccountRoles",
```

```
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListRepositories",
        "proton:ListRepositorySyncDefinitions",
        "proton:ListServiceInstanceOutputs",
        "proton:ListServiceInstanceProvisionedResources",
        "proton:ListServiceInstances",
        "proton:ListServicePipelineOutputs",
        "proton:ListServicePipelineProvisionedResources",
        "proton:ListServices",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
        "proton:ListServiceTemplates",
        "proton:ListServiceTemplateVersions",
        "proton:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSProtonServiceGitSyncServiceRolePolicy

Descrição: Política que permite ao AWS Proton sincronizar suas definições de serviço, ambiente e componente do seu repositório git com o Proton. AWS

`AWSProtonServiceGitSyncServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 04 de abril de 2023, 15:55 UTC
- Hora da edição: 04 de abril de 2023, 15:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonServiceSync",
      "Effect" : "Allow",
      "Action" : [
        "proton:GetService",
        "proton:UpdateService",
        "proton:UpdateServicePipeline",
        "proton:GetServiceInstance",
        "proton:CreateServiceInstance",
        "proton:UpdateServiceInstance",
        "proton:ListServiceInstances",
        "proton:GetComponent",
        "proton:CreateComponent",
        "proton:ListComponents",
        "proton:UpdateComponent",
        "proton:GetEnvironment",
        "proton:CreateEnvironment",
        "proton:ListEnvironments",
        "proton:UpdateEnvironment"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSProtonSyncServiceRolePolicy

Descrição: Política que permite ao AWS Proton sincronizar o conteúdo do seu repositório git com o Proton ou sincronizar o conteúdo do Proton com seus repositórios git.

`AWSProtonSyncServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 23 de novembro de 2021, 21:14 UTC
- Hora da edição: 05 de maio de 2024, 1:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SyncToProton",
      "Effect" : "Allow",
      "Action" : [
        "proton:UpdateServiceTemplateVersion",
        "proton:UpdateServiceTemplate",
        "proton:UpdateEnvironmentTemplateVersion",
        "proton:UpdateEnvironmentTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:GetServiceTemplate",
        "proton:GetEnvironmentTemplateVersion",
```

```
        "proton:GetEnvironmentTemplate",
        "proton:DeleteServiceTemplateVersion",
        "proton:DeleteEnvironmentTemplateVersion",
        "proton:CreateServiceTemplateVersion",
        "proton:CreateServiceTemplate",
        "proton:CreateEnvironmentTemplateVersion",
        "proton:CreateEnvironmentTemplate",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListServiceTemplateVersions",
        "proton:CreateEnvironmentTemplateMajorVersion",
        "proton:CreateServiceTemplateMajorVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSPurchaseOrdersServiceRolePolicy

Descrição: concede permissões para visualizar e modificar pedidos de compra no console de faturamento

`AWSPurchaseOrdersServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSPurchaseOrdersServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de maio de 2020, 18:15 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetContactInformation",
        "aws-portal:*Billing",
        "consolidatedbilling:GetAccountBillingRole",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceUnits",
        "payments:GetPaymentInstrument",
        "payments:ListPaymentPreferences",
        "purchase-orders:AddPurchaseOrder",
        "purchase-orders:DeletePurchaseOrder",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
```

```
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ModifyPurchaseOrders",
        "purchase-orders:TagResource",
        "purchase-orders:UntagResource",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus",
        "purchase-orders:ViewPurchaseOrders",
        "tax:ListTaxRegistrations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupCFGCPacksPermissionsBoundary

Descrição: a AWSQuickSetupCFGCPacksPermissionsBoundary política define a lista de permissões permitidas em uma função do IAM criada pela Configuração rápida. A Configuração rápida usa uma função criada com essa política para implantar pacotes de conformidade do AWS Config.

`AWSQuickSetupCFGCPacksPermissionsBoundary` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupCFGCPacksPermissionsBoundary` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de junho de 2024, 9:52 UTC

- Hora da edição: 26 de junho de 2024, 9:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupCFGCPacksPermissionsBoundary`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConfigurationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-CFGCPacks*"
      ]
    },
    {
      "Sid" : "ConfigurationRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-CFGCPacks*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "PutCPackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack"
      ],
      "Resource" : [
        "arn:aws:config:*:*:conformance-pack/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeCPacksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConformancePackStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConformancePacksSLRCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemsManagerSLRCreatePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EnableExplorerReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceSettingsForExplorerUpdatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupDeploymentRolePolicy

Descrição: fornece permissões para que a Configuração Rápida do AWS Systems Manager implante vários tipos de configuração. Esses tipos de configuração criam perfis e automações do IAM que configuram os serviços e os atributos da Amazon Web Services frequentemente usados com práticas recomendadas.

`AWSQuickSetupDeploymentRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupDeploymentRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de junho de 2024, 9:55 UTC
- Horário editado: 07 de setembro de 2026, 15:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDeploymentRolePolicy`

Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnRead",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "CfnTagOnMutate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
```

```
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack",
            "CreateChangeSet",
            "ExecuteChangeSet"
          ]
        }
      }
    },
    {
      "Sid" : "RGroupsGet",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CPacksRead",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConformancePacks",
        "config:DescribeConformancePackStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OpsPacksManage",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack",
        "config:DeleteConformancePack"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
```

```
          ]
        }
      },
      "Resource" : "arn:aws:config:*:*:conformance-pack/AWS-QuickSetup-*"
    },
    {
      "Sid" : "QSDocsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument",
        "ssm:UpdateDocument",
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:ListTagsForResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPackInstance-*"
      ]
    },
    {
      "Sid" : "QSDocsRead",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack*",
        "arn:aws:ssm:*::document/AWSConformancePacks-*",
        "arn:aws:ssm:*::document/AWSEC2-UpdateLaunchAgent",
        "arn:aws:ssm:*::document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
```

```
        "arn:aws:ssm:*::document/AWS-RunPatchBaselineAssociation",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableConfigRecording",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*::document/AmazonCloudWatch-ManageAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-InstallAndManageCloudWatchAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ConfigureDevOpsGuru",
        "arn:aws:ssm:*::document/AWSQuickSetupType-DeployConformancePack",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState"
      ]
    },
    {
      "Sid" : "QSAssociationsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack*",
        "arn:aws:ssm:*::document/AWSEC2-UpdateLaunchAgent",
        "arn:aws:ssm:*::document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*::document/AWS-RunPatchBaselineAssociation",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableConfigRecording",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
        "arn:aws:ssm:*::document/AmazonCloudWatch-ManageAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-InstallAndManageCloudWatchAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ConfigureDevOpsGuru",
```

```
        "arn:aws:ssm:*::document/AWSQuickSetupType-DeployConformancePack",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "EventRulesManage",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
        "events:DeleteRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/*QuickSetup-*"
      ]
    },
    {
      "Sid" : "CPacksSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "QSConfigRoleManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags",
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    },
    {
      "Sid" : "QSConfigRolePass",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
```

```
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com",
            "events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DocDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LegacyDocClean",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteDocument"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "LegacyIAMClean",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
```

```
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*QuickSetup-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "QSConfigRoleBounded",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRolePolicy",
        "iam:PutRolePolicy",
        "iam:PutRolePermissionsBoundary"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : [
            "arn:aws:iam::aws:policy/AWSQuickSetupCFGCPacksPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupCFGRecordingPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupDevOpsGuruPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupDistributorPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupSchedulerPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupSSMHostMgmtPermissionsBoundary"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    },
    {
      "Sid" : "QSConfigRoleManagedPolicies",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
```

```
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy",
            "arn:aws:iam::aws:policy/
AWSSystemsManagerEnableConfigRecordingExecutionPolicy",
            "arn:aws:iam::aws:policy/
AWSQuickSetupManagedInstanceProfileExecutionPolicy",
            "arn:aws:iam::aws:policy/AWSQuickSetupStartStopInstancesExecutionPolicy",
            "arn:aws:iam::aws:policy/AWSQuickSetupStartSSMAssociationsExecutionPolicy"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupDevOpsGuruPermissionsBoundary

Descrição: a AWSQuickSetupDevOpsGuruPermissionsBoundary política define a lista de permissões permitidas em uma função do IAM criada pela Configuração rápida. O Quick Setup usa uma função

criada com essa política para ativar e configurar o Amazon DevOps Guru. Esta política também fornece permissões para ativar o Systems Manager Explorer.

`AWSQuickSetupDevOpsGuruPermissionsBoundary` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupDevOpsGuruPermissionsBoundary` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de junho de 2024, 9:44 UTC
- Hora da edição: 26 de junho de 2024, 9:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDevOpsGuruPermissionsBoundary`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateDevOpsGuruSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudformationReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DevOpsGuruNotificationChannelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:AddNotificationChannel"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:DevOpsGuru-Default-Topic",
        "arn:aws:devops-guru:*:*:/channels"
      ]
    },
    {
      "Sid" : "DevOpsGuruConfigurationPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:UpdateResourceCollection",
        "devops-guru:UpdateServiceIntegration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DevOpsGuruDefaultSNSTopicConfigurationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:Publish",
        "sns:SetTopicAttributes",
        "sns:RemovePermission"
      ],
      "Resource" : "arn:aws:sns:*:*:DevOpsGuru-Default-Topic"
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
```

```
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupDistributorPermissionsBoundary

Descrição: QuickSetup cria funções do IAM que permitem configurar o recurso Systems Manager Distributor em seu nome e usa essa política ao criar essas funções para definir o limite de suas permissões.

`AWSQuickSetupDistributorPermissionsBoundary` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupDistributorPermissionsBoundary` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 26 de junho de 2024, 9:50 UTC
- Hora da edição: 26 de junho de 2024, 9:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDistributorPermissionsBoundary`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DistributorAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-*"
      ]
    },
    {
      "Sid" : "DistributorAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
        "iam:GetRole"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-
*"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToSSMPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils",
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore"
          ]
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-
*"
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
```

```
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "ConfigurationAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-Distributor-*",
        "arn:aws:ssm:*:*:automation-definition/UpdateCloudWatchDocument-Distributor-*",
        "arn:aws:ssm:*:*:automation-definition/AWS-ConfigureAWSPackage*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*"
      ]
    },
```

```
    {
      "Sid" : "ReadOnlyPermissionsForEnablingHostManagementBySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListTagsForResource",
        "ssm:GetAutomationExecution",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupEnableAREXExecutionPolicy

Descrição: Essa política concede permissões que permitem ao Systems Manager executar o runbook de AWSQuickSetupType-EnableAREX automação, que permite que o AWS Resource Explorer seja usado com o Systems Manager.

`AWSQuickSetupEnableAREXExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupEnableAREXExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 15 de novembro de 2024, 22:45 UTC
- Horário editado: 15 de novembro de 2024, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupEnableAREXExecutionPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadActions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListViews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowUpdateExistingIndexAndAssociateDefaultView",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:AssociateDefaultView"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateViewAndIndex",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:TagResource"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*:*:view/all-resources/*",
        "arn:aws:resource-explorer-2:*:*:index/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Type" : "QuickSetup",
          "aws:ResourceTag/Type" : "QuickSetup"
        },
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : "Type"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      },
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupEnableDHMCExecutionPolicy

Descrição: Essa política concede permissões que permitem que os diretores executem o runbook de AWSQuickSetupType-EnableDHMC automação, que ativa a configuração padrão de gerenciamento de host.

`AWSQuickSetupEnableDHMCExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupEnableDHMCExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 15 de novembro de 2024, 21:27 UTC
- Horário editado: 15 de novembro de 2024, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupEnableDHMCExecutionPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AmazonSSMManagedEC2InstanceDefaultPolicy"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting",
        "ssm:UpdateServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/ssm/managed-instance/default-ec2-
instance-management-role"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupJITNADeploymentRolePolicy

Descrição: essa política permite que a Configuração Rápida implante o tipo de configuração necessário para configurar o acesso a nós just-in-time.

`AWSQuickSetupJITNADeploymentRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupJITNADeploymentRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Tempo de criação: 17 de abril de 2025, 09:07 UTC
- Horário editado: 07 de setembro de 2026, 12:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupJITNADeploymentRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-JITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-JITNA-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack",
            "CreateChangeSet",
            "ExecuteChangeSet"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation",
```

```
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*::document/AWSQuickSetupType-SetupJITNAResources",
        "arn:aws:ssm:*::document/AWSQuickSetupType-
PropagateJustInTimeNodeAccessPolicies",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "cloudformation.amazonaws.com"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ],
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::*:policy/AWSQuickSetupManageJITNAResourcesExecutionPolicy"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-JITNA"
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-SetupJITNAResources",
            "arn:aws:ssm:*:*:association/*"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupManagedInstanceProfileExecutionPolicy

Descrição: essa política concede permissões administrativas que permitem ao Systems Manager criar um perfil de instância do IAM padrão para o recurso de Configuração Rápida e anexá-lo a instâncias do Amazon EC2 que ainda não têm um perfil de instância anexado.

`AWSQuickSetupManagedInstanceProfileExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupManagedInstanceProfileExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 15 de novembro de 2024, 21:51 UTC
- Horário editado: 03 de junho de 2026, 14:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupManagedInstanceProfileExecutionPolicy`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfilesForRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
    },
    {
```

```
      "Sid" : "DefaultInstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : "iam:AddRoleToInstanceProfile",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2AndSSMPermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ssm.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachAmazonSSMManagedInstanceCore",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AmazonSSMPatchAssociation",
            "arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess",
            "arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils",
            "arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy"
          ]
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "InstanceProfileAssociationEc2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMInstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:UpdateManagedInstanceRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagRoles",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : "arn:aws:iam::*:role/*",
```

```
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigId-*"
        }
      }
    },
    {
      "Sid" : "DenyModifyQuickSetupAutomationRoles",
      "Effect" : "Deny",
      "Action" : [
        "iam:TagRole",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
    },
    {
      "Sid" : "AutomationsStartWithTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:document/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/InvokedBy" : [
            "AWSQuickSetupType-ManageInstanceProfile"
          ],
          "aws:ResourceTag/InvokedBy" : [
            "AWSQuickSetupType-ManageInstanceProfile"
          ]
        }
      }
    },
    {
      "Sid" : "AutomationsGetPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:GetAutomationExecution",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/InvokedBy" : [
            "AWSQuickSetupType-ManageInstanceProfile"
          ]
        }
      }
    },
    {
      "Sid" : "GetQuickSetupAutomationAssumeRoles",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM",
            "AWSQuickSetupType-SSMHostMgmt",
            "AWSQuickSetupType-PatchPolicy",
            "AWSQuickSetupType-Distributor",
            "AWSQuickSetupType-CWASetup"
          ]
        }
      }
    },
    {
      "Sid" : "PassQuickSetupAutomationAssumeRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM",
            "AWSQuickSetupType-SSMHostMgmt",
            "AWSQuickSetupType-PatchPolicy",
```

```
            "AWSQuickSetupType-Distributor",
            "AWSQuickSetupType-CWASetup"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupManageJITNAResourcesExecutionPolicy

Descrição: essa política concede permissões para habilitar o acesso do Systems Manager a nós just-in-time.

`AWSQuickSetupManageJITNAResourcesExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupManageJITNAResourcesExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 17 de abril de 2025, 21:37 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupManageJITNAResourcesExecutionPolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateJustInTimeAccessServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/justintimeaccess.ssm.amazonaws.com/
AWSServiceRoleForSystemsManagerJustInTimeAccess"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "justintimeaccess.ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateSystemsManagerNotificationServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/notifications.ssm.amazonaws.com/
AWSServiceRoleForSystemsManagerNotifications"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "notifications.ssm.amazonaws.com"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SSM-JustInTimeAccessTokenRole",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::*:policy/
AWSSystemsManagerJustInTimeAccessTokenPolicy"
        }
      }
    },
    {
      "Sid" : "IAMRoleManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole",
        "iam:TagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SSM-JustInTimeAccessTokenRole"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ]
        }
      }
    },
    {
      "Sid" : "ServiceSettingsManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
```

```
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/just-in-time-access/identity-provider"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupPatchPolicyBaselineAccess

Descrição: Fornece permissões somente para leitura para acessar as linhas de base do patch que foram configuradas por um administrador na organização atual Conta da AWS ou na organização usando a Configuração rápida.

`AWSQuickSetupPatchPolicyBaselineAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupPatchPolicyBaselineAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de junho de 2024, 9:38 UTC
- Hora da edição: 26 de junho de 2024, 9:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QuickSetupPatchingBaselineOverridesS3SameAccountReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "QuickSetupPatchingBaselineOverridesS3OrganizationReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalOrgID" : [
            "${aws:ResourceOrgID}"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupPatchPolicyDeploymentRolePolicy

Descrição: fornece permissões que permitem que a Configuração Rápida crie recursos associados a uma configuração de política de patches.

`AWSQuickSetupPatchPolicyDeploymentRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupPatchPolicyDeploymentRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de junho de 2024, 9:57 UTC
- Horário editado: 04 de setembro de 2026, 08:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyDeploymentRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "CfnRead",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackDriftDetectionStatus",
      "cloudformation:ListStacks"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "CfnManage",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
      "cloudformation:UpdateStack",
      "cloudformation:DeleteStack",
      "cloudformation:CreateChangeSet",
      "cloudformation:DeleteChangeSet",
      "cloudformation:ExecuteChangeSet",
      "cloudformation:DescribeChangeSet",
      "cloudformation:DescribeStackResourceDrifts",
      "cloudformation:DetectStackDrift",
      "cloudformation:DetectStackResourceDrift"
    ],
    "Resource" : [
      "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
    ]
  },
  {
    "Sid" : "RGroupsGet",
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:GetGroupQuery"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
```

```
      "Sid" : "S3BucketsList",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AccessLogsBucketManage",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:Put*",
        "s3:Get*",
        "s3:List*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:s3:::aws-quicksetup-patchpolicy-access-log-*"
      ]
    },
    {
      "Sid" : "LambdaManage",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:UpdateFunction*",
        "lambda:GetFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:DeleteFunction",
```

```
        "lambda:InvokeFunction",
        "lambda:UntagResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      },
      "Resource" : [
        "arn:aws:lambda:*:*:function:baseline-overrides-*",
        "arn:aws:lambda:*:*:function:delete-name-tags-*"
      ]
    },
    {
      "Sid" : "LogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LogGroupsManage",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource",
        "logs:PutRetentionPolicy",
        "logs:DeleteLogGroup",
        "logs:ListTagsForResource",
        "logs:UntagResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
```

```
        }
      },
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/baseline-overrides-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/delete-name-tags-*"
      ]
    },
    {
      "Sid" : "QSDocsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument",
        "ssm:UpdateDocument",
        "ssm:DescribeDocument",
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:ListTagsForResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/QuickSetup-*"
      ]
    },
    {
      "Sid" : "QSDocsGet",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-RunPatchBaseline"
      ]
```

```
    },
    {
      "Sid" : "QSAssociationsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-RunPatchBaseline",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "ConfigRoleManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole",
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "ConfigRolePassToSSM",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConfigRolePassToLambda",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DocDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LegacyDocClean",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteDocument"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "LegacyIAMClean",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*QuickSetup-*",
      "Condition" : {
```

```
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "ConfigRoleBoundedManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePolicy",
        "iam:PutRolePermissionsBoundary"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AWSQuickSetupPatchPolicyPermissionsBoundary"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "CfnTagOnMutate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
```

```
            "CreateStack",
            "UpdateStack",
            "CreateChangeSet",
            "ExecuteChangeSet"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupPatchPolicyLambdaExecutionPolicy

Descrição: Concede permissões para gerenciar associações de gerentes de estado para operações de limpeza automatizadas quando as configurações de configuração rápida são excluídas.

`AWSQuickSetupPatchPolicyLambdaExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupPatchPolicyLambdaExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de junho de 2026, 14:12 UTC
- Horário editado: 03 de junho de 2026, 14:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyLambdaExecutionPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageSSMAssociations",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions",
        "ssm:UpdateAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-*"
      ]
    },
    {
      "Sid" : "PassQuickSetupAutomationRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupPatchPolicyPermissionsBoundary

Descrição: QuickSetup cria funções do IAM que permitem configurar o recurso Systems Manager Patch Manager em seu nome e usa essa política ao criar essas funções para definir o limite de suas permissões.

`AWSQuickSetupPatchPolicyPermissionsBoundary` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupPatchPolicyPermissionsBoundary` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de junho de 2024, 9:46 UTC
- Horário editado: 05 de março de 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyPermissionsBoundary`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PatchingAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
      ]
    },
    {
      "Sid" : "PatchingAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
        "iam:GetRole"
      ],
      "Condition" : {
        "StringLike" : {
```

```
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess"
          ]
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
```

```
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "CreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ManagedInstanceRoleUpdatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateManagedInstanceRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "InstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "InstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "InstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "SSMAssociationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions",
        "ssm:UpdateAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "BaselineS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:Put*",
        "s3:Get*",
        "s3:List*",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteBucket"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      },
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*"
    },
    {
```

```
      "Sid" : "PatchingFunctionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:baseline-overrides-*",
        "arn:aws:lambda:*:*:function:delete-name-tags-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "LoggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/baseline-overrides-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/delete-name-tags-*"
      ]
    },
    {
      "Sid" : "SSMTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    },
```

```
    {
      "Sid" : "EC2TaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    },
    {
      "Sid" : "RoleTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigId-*"
        }
      }
    },
    {
      "Sid" : "PatchingReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetPatchBaseline",
        "ssm:GetInventory",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeAssociation",
        "ssm:GetAutomationExecution",
        "ssm:ListTagsForResource",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "PatchingAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-EnableExplorer*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RunPatchBaseline*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/QuickSetup-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWS-EnableExplorer*",
        "arn:aws:ssm:*:*:document/AWS-RunPatchBaseline*",
        "arn:aws:ssm:*:*:document/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ]
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
```

```
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupPatchPolicyTagManagementExecutionPolicy

Descrição: concede permissões para rastrear quais instâncias são gerenciadas pelas configurações da política de patch do Quick Setup por meio de marcação automática e coleta de inventário.

`AWSQuickSetupPatchPolicyTagManagementExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupPatchPolicyTagManagementExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de junho de 2026, 14:12 UTC
- Horário editado: 03 de junho de 2026, 14:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyTagManagementExecutionPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GetSSMInventory",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetInventory"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageSSMManagedInstanceTags",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    },
    {
      "Sid" : "ManageEC2InstanceTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
```

```
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupSchedulerPermissionsBoundary

Descrição: a AWSQuickSetupSchedulerPermissionsBoundary política define a lista de permissões permitidas em uma função do IAM criada pela Configuração rápida. A Configuração Rápida usa um perfil criado com esta política para habilitar e configurar operações programadas em instâncias do Amazon EC2 e outros recursos.

`AWSQuickSetupSchedulerPermissionsBoundary` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupSchedulerPermissionsBoundary` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 26 de junho de 2024, 9:53 UTC
- Hora da edição: 26 de junho de 2024, 9:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSchedulerPermissionsBoundary`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConfigurationAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-Scheduler-*"
      ]
    },
    {
      "Sid" : "ConfigurationAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-Scheduler-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "SystemsManagerCalendarReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCalendarState"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-ChangeCalendar-*"
      ]
    },
    {
      "Sid" : "EC2ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2StartStopPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AutomationStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
```

```
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
StartStateManagerAssociations-*"
      ]
    },
    {
      "Sid" : "AssociationsStartOncePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAssociationsOnce"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupSSMDeploymentRolePolicy

Descrição: essa política concede permissões administrativas que permitem à Configuração Rápida criar os recursos usados durante o processo de integração do Systems Manager.

`AWSQuickSetupSSMDeploymentRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupSSMDeploymentRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 15 de novembro de 2024, 22:53 UTC
- Horário editado: 07 de setembro de 2026, 12:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentRolePolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
```

```
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-SSM-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-SSM-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack",
            "CreateChangeSet",
            "ExecuteChangeSet"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
```

```
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ],
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:DeleteFunction",
        "lambda:UpdateFunction*"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableAREX",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableDHMC",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
```

```
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-LifecycleManagement-*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/
AWSQuickSetupSSMLifecycleManagementExecutionPolicy"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupSSMManageResourcesExecutionPolicy"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
AdministrationRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
ExecutionRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
OperationalAccountAdministrationRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-Automation-DiagnosisBucketPolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-
AdministrationRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
      ],
      "Condition" : {
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-EnableAREX",
            "arn:aws:ssm:*::document/AWSQuickSetupType-EnableDHMC",
            "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
            "arn:aws:ssm:*::document/AWS-EnableExplorer",
            "arn:aws:ssm:*:*:association/*"
          ]
        },
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-LifecycleManagement*"
      ],
      "Condition" : {
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle-*"
          ]
        },
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "lambda:TagResource",
      "Resource" : [
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QuickSetup*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        },
        "StringLike" : {
          "aws:RequestTag/QuickSetupDocumentVersionName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QuickSetup*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        },
        "StringLike" : {
          "aws:RequestTag/QuickSetupDocumentVersionName" : "*"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : "arn:aws:ssm:*::document/AWSQuickSetupType-SSM-ManageResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions",
        "ssm:DescribeAssociationExecutionTargets",
        "ssm:GetAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupSSMDeploymentS3BucketRolePolicy

Descrição: Essa política concede permissões para listar todos os buckets do S3 em uma conta e para gerenciar e recuperar informações sobre buckets específicos na conta principal que são gerenciados por meio de modelos. AWS CloudFormation

`AWSQuickSetupSSMDeploymentS3BucketRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupSSMDeploymentS3BucketRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 15 de novembro de 2024, 22:01 UTC
- Horário editado: 15 de novembro de 2024, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentS3BucketRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketTagging",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      },
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupSSMHostMgmtPermissionsBoundary

Descrição: a Configuração Rápida cria perfis do IAM que permitem configurar o recurso de Configuração Rápida do Host Manager em seu nome e usa essa política ao criar esses perfis para definir o limite de suas permissões.

`AWSQuickSetupSSMHostMgmtPermissionsBoundary` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupSSMHostMgmtPermissionsBoundary` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de junho de 2024, 9:48 UTC
- Hora da edição: 26 de junho de 2024, 9:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMHostMgmtPermissionsBoundary`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HostManagementAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
      ]
    },
    {
      "Sid" : "HostManagementAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
```

```
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AmazonSSMPatchAssociation"
          ]
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
```

```
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "ConfigurationAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-HostMgmt-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
CreateAndAttachIAMToInstance-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
UpdateExistingInstanceProfile-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
InstallAndManageCloudWatchDocument-*",
        "arn:aws:ssm:*:*:automation-definition/UpdateCloudWatchDocument-*",
        "arn:aws:ssm:*:*:automation-definition/AWSEC2-UpdateLaunchAgent-*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/AWS-GatherSoftwareInventory*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RunPatchBaselineAssociation*",
        "arn:aws:ssm:*:*:automation-definition/AWS-UpdateSSMAgent*"
      ]
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingHostManagementBySSM",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:ListTagsForResource",
        "ssm:GetAutomationExecution",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupSSMLifecycleManagementExecutionPolicy

Descrição: a política concede permissões administrativas que permitem que a Configuração Rápida execute um recurso AWS CloudFormation personalizado em eventos do ciclo de vida durante a implantação da Configuração Rápida no Systems Manager.

`AWSQuickSetupSSMLifecycleManagementExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupSSMLifecycleManagementExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 15 de novembro de 2024, 21:55 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMLifecycleManagementExecutionPolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-SSM-ManageResources*",
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-SSM-ManageResources*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : "AWSQuickSetupType-SSM",
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupSSMManageResourcesExecutionPolicy

Descrição: essa política concede permissões para que o Systems Manager crie pré-requisitos, como os perfis do IAM necessários para a integração do Systems Manager.

`AWSQuickSetupSSMManageResourcesExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupSSMManageResourcesExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 15 de novembro de 2024, 22:49 UTC
- Horário editado: 15 de novembro de 2024, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMManageResourcesExecutionPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM",
          "aws:RequestTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:UpdateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy"
          ]
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupEnableDHMCExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupManagedInstanceProfileExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupEnableAREXExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:ListBucketVersions",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupStartSSMAssociationsExecutionPolicy

Descrição: Essa política concede permissões que permitem que os diretores executem o runbook de AWSQuickSetupType-StartSSMAssociations automação, que inicia as associações de gerentes estaduais.

`AWSQuickSetupStartSSMAssociationsExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupStartSSMAssociationsExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 08 de agosto de 2025, 12:04 UTC
- Horário editado: 05 de março de 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupStartSSMAssociationsExecutionPolicy`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ChangeCalendarState*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
            "arn:aws:ssm:*:*:automation-execution/*",
            "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ChangeCalendarState*"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSetupStartStopInstancesExecutionPolicy

Descrição: A política gerenciada AWSQuickSetupStartStopInstancesExecutionPolicy fornece permissões para que o Quick Setup inicie e interrompa instâncias do Amazon EC2 de acordo com um cronograma. Essa política é usada com o tipo de configuração do programador da Configuração Rápida.

`AWSQuickSetupStartStopInstancesExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSetupStartStopInstancesExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 08 de agosto de 2025, 12:04 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupStartStopInstancesExecutionPolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
```

```
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeRegions",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCalendarState"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AWSQuickSetup-ChangeCalendar*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAssociationsOnce",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ApplyInstanceState*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "ssm.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
            "arn:aws:ssm:*:*:association/*"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSightAssetBundleExportPolicy

Descrição: fornece o conjunto de permissões necessárias para realizar operações de exportação QuickSight de pacotes de ativos

`AWSQuickSightAssetBundleExportPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSightAssetBundleExportPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de março de 2024, 21:31 UTC
- Hora da edição: 27 de março de 2024, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleExportPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TagReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListTagsForResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:*/*"
    },
    {
      "Sid" : "DashboardReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dashboard/*"
    },
    {
      "Sid" : "AnalysisReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:analysis/*"
    },
    {
      "Sid" : "DataSetReadAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:ListRefreshSchedules",
        "quicksight:DescribeDataSetPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*"
    },
    {
      "Sid" : "DataSourceReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*"
    },
    {
      "Sid" : "ThemeReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:theme/*"
    },
    {
      "Sid" : "VPCConnectionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeVPCConnection",
        "quicksight:ListVPCConnections"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcConnection/*"
    },
    {
      "Sid" : "RefreshScheduleReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeRefreshSchedule"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*/refresh-schedule/*"
    },
    {
      "Sid" : "AssetBundleExportOperations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAssetBundleExportJob",
        "quicksight:ListAssetBundleExportJobs",
        "quicksight:StartAssetBundleExportJob"
      ],
      "Resource" : "arn:aws:quicksight:*:*:asset-bundle-export-job/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSightAssetBundleImportPolicy

Descrição: fornece o conjunto de permissões necessárias para realizar operações de importação QuickSight de pacotes de ativos

`AWSQuickSightAssetBundleImportPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSightAssetBundleImportPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de março de 2024, 21:40 UTC
- Hora da edição: 27 de março 2024, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleImportPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TagWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListTagsForResource",
        "quicksight:TagResource",
        "quicksight:UntagResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:*/*"
    },
    {
      "Sid" : "DashboardWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDashboard",
        "quicksight:DeleteDashboard",
        "quicksight:DescribeDashboard",
        "quicksight:UpdateDashboard",
        "quicksight:UpdateDashboardPublishedVersion",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:UpdateDashboardPermissions",
        "quicksight:UpdateDashboardLinks"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dashboard/*"
    },
    {
      "Sid" : "AnalysisWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateAnalysis",
```

```
        "quicksight:DeleteAnalysis",
        "quicksight:DescribeAnalysis",
        "quicksight:UpdateAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:UpdateAnalysisPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:analysis/*"
    },
    {
      "Sid" : "DataSetWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSet",
        "quicksight:DeleteDataSet",
        "quicksight:DescribeDataSet",
        "quicksight:PassDataSet",
        "quicksight:UpdateDataSet",
        "quicksight:DeleteDataSetRefreshProperties",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:PutDataSetRefreshProperties",
        "quicksight:UpdateDataSetPermissions",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:ListRefreshSchedules"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*"
    },
    {
      "Sid" : "DataSourceWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSource",
        "quicksight:DescribeDataSource",
        "quicksight:DeleteDataSource",
        "quicksight:PassDataSource",
        "quicksight:UpdateDataSource",
        "quicksight:UpdateDataSourcePermissions",
        "quicksight:DescribeDataSourcePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*"
    },
    {
      "Sid" : "ThemeWriteAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "quicksight:CreateTheme",
        "quicksight:DeleteTheme",
        "quicksight:DescribeTheme",
        "quicksight:UpdateTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:UpdateThemePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:theme/*"
    },
    {
      "Sid" : "RefreshScheduleWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateRefreshSchedule",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DeleteRefreshSchedule",
        "quicksight:UpdateRefreshSchedule"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*/refresh-schedule/*"
    },
    {
      "Sid" : "VPCConnectionWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListVPCConnections",
        "quicksight:CreateVPCConnection",
        "quicksight:DescribeVPCConnection",
        "quicksight:DeleteVPCConnection",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcConnection/*"
    },
    {
      "Sid" : "AssetBundleImportOperations",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAssetBundleImportJob",
        "quicksight:ListAssetBundleImportJobs",
        "quicksight:StartAssetBundleImportJob"
      ],
      "Resource" : "arn:aws:quicksight:*:*:asset-bundle-import-job/*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuicksightAthenaAccess

Descrição: acesso do QuickSight à API do Athena e aos buckets do S3 usados para resultados de consultas do Athena

`AWSQuicksightAthenaAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuicksightAthenaAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 09 de dezembro de 2016, 2:31 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess`

Versão da política

Versão da política: v13 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetQueryExecution",
        "athena:CancelQueryExecution",
        "athena:GetCatalogs",
        "athena:GetExecutionEngine",
        "athena:GetExecutionEngines",
        "athena:GetNamespace",
        "athena:GetNamespaces",
        "athena:GetQueryExecution",
        "athena:GetQueryExecutions",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetTable",
        "athena:GetTables",
        "athena:ListQueryExecutions",
        "athena:RunQuery",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:ListWorkGroups",
        "athena:ListEngineVersions",
        "athena:GetWorkGroup",
        "athena:GetDataCatalog",
        "athena:GetDatabase",
        "athena:GetTableMetadata",
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
```

```
        "glue:DeleteDatabase",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-athena-query-results-*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSightDescribeRDS

Descrição: Permitir QuickSight descrever os recursos do RDS

`AWSQuickSightDescribeRDS` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSightDescribeRDS` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 10 de novembro de 2015, 23:24 UTC
- Hora da edição: 10 de novembro de 2015, 23:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSightDescribeRedshift

Descrição: Permitir QuickSight descrever os recursos do Redshift

`AWSQuickSightDescribeRedshift` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSightDescribeRedshift` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço

- Hora da criação: 10 de novembro de 2015, 23:25 UTC
- Hora da edição: 10 de novembro de 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "redshift:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSightElasticsearchPolicy

Descrição: Fornece acesso aos recursos do Amazon Elasticsearch da Amazon QuickSight

`AWSQuickSightElasticsearchPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSightElasticsearchPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 09 de setembro de 2020, 17:27 UTC
- Hora da edição: 07 de setembro de 2021, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "es:ListDomainNames",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:DescribeElasticsearchDomain",
        "es:DescribeDomain"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpPost",
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/_opendistro/_sql",
        "arn:aws:es:*:*:domain/*/_plugin/_sql"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSightIoTAnalyticsAccess

Descrição: QuickSight Ofereça acesso somente para leitura aos conjuntos de dados do IoT Analytics

`AWSQuickSightIoTAnalyticsAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSightIoTAnalyticsAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2017, 17:00 UTC
- Hora da edição: 29 de novembro de 2017, 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iotanalytics:ListDatasets",
        "iotanalytics:DescribeDataset",
        "iotanalytics:GetDatasetContent"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSightListIAM

Descrição: QuickSight Permitir listar entidades do IAM

`AWSQuickSightListIAM` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSightListIAM` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 10 de novembro de 2015, 23:25 UTC
- Hora da edição: 10 de novembro de 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:List*"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuicksightOpenSearchPolicy

Descrição: Fornece acesso aos OpenSearch recursos da Amazon a partir da Amazon QuickSight

`AWSQuicksightOpenSearchPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuicksightOpenSearchPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 07 de setembro de 2021, 23:26 UTC
- Hora da edição: 07 de setembro de 2021, 23:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "es:ListDomainNames",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:DescribeDomain"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpPost",
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/_opendistro/_sql",
        "arn:aws:es:*:*:domain/*/_plugin/_sql"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSightSageMakerPolicy

Descrição: Fornece acesso aos SageMaker recursos da Amazon a partir da Amazon QuickSight

`AWSQuickSightSageMakerPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSightSageMakerPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 17 de janeiro de 2020, 17:18 UTC
- Hora da edição: 30 de outubro de 2023, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "SageMakerTransformJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:CreateTransformJob"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:transform-job/quicksight-auto-generated-*"
    },
    {
      "Sid" : "SageMakerModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListModels",
        "sagemaker:DescribeModel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ObjectReadAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::quicksight-ml.*",
        "arn:aws:s3:::sagemaker*"
      ]
    },
    {
      "Sid" : "S3ObjectUpdateAccess",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : "arn:aws:s3:::sagemaker*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3BucketReadAccess",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::sagemaker*"
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSightSecretsManagerWriteAccess

Descrição: Política usada pelo QuickSight para criar AWS segredos no Secrets Manager e anexar políticas de recursos aos QuickSight segredos existentes.

`AWSQuickSightSecretsManagerWriteAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSightSecretsManagerWriteAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 22 de maio de 2025, 01:22 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSecretsManagerWriteAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "quicksight",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "secretsmanager:Name" : "quicksight!*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSightSecretsManagerWritePolicy

Descrição: Política usada pelo QuickSight para criar AWS segredos no Secrets Manager e anexar políticas de recursos aos QuickSight segredos existentes.

`AWSQuickSightSecretsManagerWritePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSightSecretsManagerWritePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 12 de maio de 2025, 19:22 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightSecretsManagerWritePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
```

```
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "quicksight",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "secretsmanager:Name" : "quicksight!*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSQuickSightTimestreamPolicy

Descrição: AWS QuickSight acesso às APIs do AWS Timestream. Os clientes podem anexar essa política à AWS QuickSight função para permitir a recuperação de dados e metadados.

`AWSQuickSightTimestreamPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSQuickSightTimestreamPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 30 de setembro de 2020, 21:47 UTC
- Hora da edição: 30 de setembro de 2020, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:Select",
        "timestream:CancelQuery",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase",
        "timestream:SelectValues",
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSReachabilityAnalyzerServiceRolePolicy

Descrição: permite que o VPC Reachability Analyzer acesse AWS recursos e se integre às AWS organizações em seu nome.

`AWSReachabilityAnalyzerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 23 de novembro de 2022, 17:12 UTC
- Horário editado: 14 de agosto de 2026, 17:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReachabilityAnalyzerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:GetTransitGatewayPolicyTableEntries",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeAddresses",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallMetadata",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "tag:GetResources",
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApigatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
```

```
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSRefactoringToolkitFullAccess

Descrição: Essa política concede permissão para usar AWS serviços com a extensão AWS Toolkit for .NET Refactoring para Microsoft Visual Studio. Ele deve ser anexado a um AWS perfil local. A política permite o upload de artefatos do aplicativo e o download dos artefatos resultantes do Amazon S3. Ele permite criar aplicativos em uma imagem de contêiner usando, armazenar AWS CodeBuild e recuperar as imagens do Amazon Elastic Container Registry (Amazon ECR). Além disso, permite a implantação do aplicativo em serviços de contêiner, AWS como o Amazon Elastic Container Service (Amazon ECS), a criação opcional de recursos de VPC, a conexão opcional à infraestrutura existente, como o AWS Directory Service, e outros serviços relacionados.

`AWSRefactoringToolkitFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSRefactoringToolkitFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de outubro de 2022, 16:41 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a2c:GetContainerizationJobDetails",
        "a2c:GetDeploymentJobDetails",
        "a2c:StartContainerizationJob",
        "a2c:StartDeploymentJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:*:cloudformation:*:*:stack/a2c-app-*",
        "arn:*:cloudformation:*:*:stack/a2c-build-*",
        "arn:*:cloudformation:*:*:stack/application-transformation-app-*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:UpdateProject"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:StartBuild"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-transformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "AuthorizeSecurityGroupIngress",
            "CreateInternetGateway",
            "CreateKeyPair",
            "CreateRoute",
```

```
            "CreateRouteTable",
            "CreateSubnet",
            "CreateVpc"
          ]
        },
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-transformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
```

```
        "ec2:ModifyVpcAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
        "ecr:GetRepositoryPolicy",
```

```
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTaskDefinition"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "a2c-sidecar"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "application-transformation-sidecar"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ecs.amazonaws.com"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "a2c-generated"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "application-transformation"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:GetParameters",
        "ssm:PutParameter",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/a2c-generated-check-ecs-slr-*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:DescribeSessions",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/refactoringtoolkit*",
        "arn:aws:s3:::*/a2c-generated*",
        "arn:aws:s3:::*/application-transformation*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "application-transformation",
            "refactoringtoolkit"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "clouddirectory:ListDirectories",
        "codebuild:BatchGetProjects",
```

```
        "codebuild:BatchGetBuilds",
        "ds:DescribeDirectories",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ecr:DescribeImages",
        "ecr:DescribeRepositories",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTasks",
        "ecs:ListTagsForResource",
        "ecs:ListTasks",
        "iam:ListRoles",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning",
        "s3:ListAllMyBuckets",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore",
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore/*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "application-transformation:StartPortingCompatibilityAssessment",
        "application-transformation:GetPortingCompatibilityAssessment",
        "application-transformation:StartPortingRecommendationAssessment",
        "application-transformation:GetPortingRecommendationAssessment",
        "application-transformation:PutLogData",
        "application-transformation:PutMetricData",
        "application-transformation:StartContainerization",
        "application-transformation:GetContainerization",
        "application-transformation:StartDeployment",
        "application-transformation:GetDeployment"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
```

```
          "ecr:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSRefactoringToolkitSidecarPolicy

Descrição: Essa política deve ser usada pelo Amazon ECS Tasks criado para testar aplicativos AWS usando a extensão AWS Toolkit for .NET Refactoring para Microsoft Visual Studio. A política

concede acesso para baixar artefatos de aplicativos do Amazon S3, comunicar o status da tarefa usando o AWS Systems Manager e outros serviços necessários.

`AWSRefactoringToolkitSidecarPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSRefactoringToolkitSidecarPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de outubro de 2022, 16:41 UTC
- Hora da edição: 29 de outubro de 2022, 22:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmMessagesAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenControlChannel",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssmmessages:CreateDataChannel"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/refactoringtoolkit*"
    },
    {
      "Sid" : "S3ListBucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : "refactoringtoolkit*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSrePostPrivateCloudWatchAccess

Descrição: Fornece acesso privado ao Re:post para publicar dados de métricas CloudWatch

`AWSrePostPrivateCloudWatchAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 15 de novembro de 2023, 16:37 UTC
- Hora da edição: 15 de novembro de 2023, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchPublishMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/rePostPrivate",
            "AWS/Usage"
```

```
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSRepostSpaceSupportOperationsPolicy

Descrição: esta política permite que o serviço re:Post Space crie, gerencie e resolva casos de suporte criados via aplicação Space.

`AWSRepostSpaceSupportOperationsPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSRepostSpaceSupportOperationsPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de novembro de 2023, 21:52 UTC
- Hora da edição: 26 de novembro de 2023, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSResilienceHubAsssessmentExecutionPolicy

Descrição: Política para a função de serviço do AWS Resilience Hub, que permite o acesso a outros AWS serviços para executar a avaliação.

`AWSResilienceHubAsssessmentExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSResilienceHubAsssessmentExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de junho de 2023, 12:32 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFullResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ValidateTemplate",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "datasync:DescribeTask",
        "datasync:ListLocations",
        "datasync:ListTasks",
```

```
        "devops-guru:ListMonitoredResources",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "docdb-elastic:GetCluster",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:ListTagsForResource",
        "drs:DescribeJobs",
        "drs:DescribeSourceServers",
        "drs:GetReplicationConfiguration",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleets",
        "ec2:DescribeHosts",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ecr:DescribeRegistry",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "elasticache:DescribeCacheClusters",
```

```
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeServerlessCaches",
        "elasticache:DescribeServerlessCacheSnapshots",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "fis:GetExperiment",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fis:ListExperimentResolvedTargets",
        "fsx:DescribeFileSystems",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:ListAliases",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSnapshots",
        "rds:DescribeGlobalClusters",
        "rds:ListTagsForResource",
        "resource-groups:GetGroup",
        "resource-groups:ListGroupResources",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
```

```
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:ListBucket",
        "servicecatalog:GetApplication",
        "servicecatalog:ListAssociatedResources",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "ssm:DescribeAutomationExecutions",
        "states:DescribeStateMachine",
        "states:ListStateMachineVersions",
        "states:ListStateMachineAliases",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSResilienceHubApiGatewayStatement",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans"
      ]
    },
    {
      "Sid" : "AWSResilienceHubS3ArtifactStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::aws-resilience-hub-artifacts-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubS3AccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubCloudWatchStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "ResilienceHub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubSSMStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath"
      ],
```

```
      "Resource" : "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSResilienceHubResilienceTestingPolicy

Descrição: Política para a função de serviço do AWS Resilience Hub, que permite o acesso ao AWS Fault Injection Service para iniciar o teste de resiliência.

`AWSResilienceHubResilienceTestingPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSResilienceHubResilienceTestingPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 31 de julho de 2026, 22:27 UTC
- Horário editado: 31 de julho de 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubResilienceTestingPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFISActionStatement",
      "Effect" : "Allow",
      "Action" : "fis:CreateExperimentTemplate",
      "Resource" : "arn:aws:fis:*:*:action/*"
    },
    {
      "Sid" : "AWSResilienceHubFISCreateExperimentTemplateStatement",
      "Effect" : "Allow",
      "Action" : "fis:CreateExperimentTemplate",
      "Resource" : "arn:aws:fis:*:*:experiment-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedBy" : "resiliencehub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubFISStartExperimentFromTemplateStatement",
      "Effect" : "Allow",
      "Action" : "fis:StartExperiment",
      "Resource" : "arn:aws:fis:*:*:experiment-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/managedBy" : "resiliencehub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubFISStartExperimentStatement",
      "Effect" : "Allow",
      "Action" : "fis:StartExperiment",
      "Resource" : "arn:aws:fis:*:*:experiment/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/managedBy" : "resiliencehub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubFISExperimentStatement",
      "Effect" : "Allow",
      "Action" : [
        "fis:GetExperiment",
        "fis:StopExperiment",
        "fis:ListExperimentResolvedTargets"
      ],
      "Resource" : "arn:aws:fis:*:*:experiment/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/managedBy" : "resiliencehub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubFISExperimentTemplateStatement",
      "Effect" : "Allow",
      "Action" : [
        "fis:CreateTargetAccountConfiguration",
        "fis:DeleteExperimentTemplate"
      ],
      "Resource" : "arn:aws:fis:*:*:experiment-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/managedBy" : "resiliencehub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubFISPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "fis.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AWSResilienceHubFISTagResourceStatement",
      "Effect" : "Allow",
      "Action" : "fis:TagResource",
      "Resource" : [
        "arn:aws:fis:*:*:experiment-template/*",
        "arn:aws:fis:*:*:experiment/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedBy" : "resiliencehub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubRegionSwitchStatement",
      "Effect" : "Allow",
      "Action" : [
        "arc-region-switch:ListPlanExecutions",
        "arc-region-switch:GetPlanExecution"
      ],
      "Resource" : "arn:aws:arc-region-switch::*:plan/*:*"
    },
    {
      "Sid" : "AWSResilienceHubFISCreateSLRStatement",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "fis.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubCloudWatchAlarmStatement",
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarmHistory",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSResilienceHubServiceRolePolicy

Descrição: permite que o AWS Resilience Hub acesse recursos em sua conta para descoberta, avaliação e gerenciamento de resiliência.

`AWSResilienceHubServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 28 de maio de 2026, 17:42 UTC
- Horário editado: 06 de julho de 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResilienceHubServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubOrganizationsReadStatement",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots",
        "organizations:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSResilienceHubV2AssessmentExecutionPolicy

Descrição: permite que o AWS Resilience Hub acesse recursos em sua conta para descoberta, avaliação e gerenciamento de resiliência. Essa política concede permissões de somente leitura com caracteres curinga que podem incluir informações confidenciais na saída.

`AWSResilienceHubV2AssessmentExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSResilienceHubV2AssessmentExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 17 de junho de 2026, 22:57 UTC
- Horário editado: 17 de junho de 2026, 22:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubV2AssessmentExecutionPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubV2ReadResourceConfigStatement",
      "Effect" : "Allow",
      "Action" : [
        "acm:Describe*",
        "acm:List*",
        "application-autoscaling:Describe*",
        "application-autoscaling:GetPredictiveScalingForecast",
        "application-autoscaling:ListTagsForResource",
        "arc-region-switch:Get*",
        "arc-region-switch:List*",
        "arc-zonal-shift:Get*",
        "arc-zonal-shift:List*",
        "autoscaling:Describe*",
        "autoscaling:GetPredictiveScalingForecast",
```

```
        "backup:Describe*",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:List*",
        "cloudformation:Describe*",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:List*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "config:Describe*",
        "config:GetStoredQuery",
        "config:List*",
        "datasync:Describe*",
        "datasync:List*",
        "dlm:Get*",
        "docdb-elastic:Get*",
        "docdb-elastic:List*",
        "drs:Describe*",
        "drs:Get*",
        "drs:List*",
        "ds:Describe*",
        "dsql:Get*",
        "dsql:List*",
        "dynamodb:Describe*",
        "dynamodb:GetResourcePolicy",
        "dynamodb:List*",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeClientVpnConnections",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleets",
```

```
        "ec2:DescribeFlowLogs",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ecr:Describe*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
```

```
        "eks:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticfilesystem:Describe*",
        "elasticfilesystem:ListTagsForResource",
        "elasticloadbalancing:Describe*",
        "events:Describe*",
        "events:List*",
        "firehose:Describe*",
        "firehose:List*",
        "fis:Get*",
        "fis:List*",
        "fsx:Describe*",
        "fsx:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "iam:GetInstanceProfile",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListRoleTags",
        "kafka:Describe*",
        "kafka:GetClusterPolicy",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kinesis:Describe*",
        "kinesis:List*",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
```

```
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
        "memorydb:Describe*",
        "memorydb:List*",
        "network-firewall:Describe*",
        "network-firewall:List*",
        "qldb:Describe*",
        "qldb:List*",
        "ram:Get*",
        "ram:List*",
        "rds:Describe*",
        "rds:List*",
        "redshift:Describe*",
        "redshift:List*",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "route53-recovery-cluster:Get*",
        "route53-recovery-cluster:List*",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:Get*",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53domains:Check*",
        "route53domains:List*",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3:ListBucket",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecrets",
        "servicecatalog:GetApplication",
        "servicecatalog:ListAssociatedResources",
        "shield:Describe*",
        "shield:Get*",
        "shield:List*",
        "sns:GetDataProtectionPolicy",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:List*",
        "sqs:GetQueueAttributes",
```

```
        "sqs:GetQueueUrl",
        "sqs:List*",
        "ssm:Describe*",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetMaintenanceWindow",
        "ssm:GetParameters",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:List*",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:List*",
        "states:Describe*",
        "states:List*",
        "tag:GetResources",
        "vpc-lattice:Get*",
        "vpc-lattice:List*",
        "wafv2:Get*",
        "wafv2:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSResilienceHubApiGatewayStatement",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/domainnames/*"
      ]
    },
    {
      "Sid" : "AWSResilienceHubS3AccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
```

```
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSResourceAccessManagerFullAccess

Descrição: Fornece acesso total ao AWS Resource Access Manager

`AWSResourceAccessManagerFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSResourceAccessManagerFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 04 de junho de 2019, 17:28 UTC

- Hora da edição: 04 de junho de 2019, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSResourceAccessManagerReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao AWS Resource Access Manager.

`AWSResourceAccessManagerReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSResourceAccessManagerReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de dezembro de 2019, 20:58 UTC
- Hora da edição: 09 de dezembro de 2019, 20:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:Get*",
        "ram:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSResourceAccessManagerResourceShareParticipantAccess

Descrição: fornece acesso às APIs do AWS Resource Access Manager necessárias para um participante do compartilhamento de recursos.

`AWSResourceAccessManagerResourceShareParticipantAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSResourceAccessManagerResourceShareParticipantAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de dezembro de 2019, 20:41 UTC
- Hora da edição: 09 de dezembro de 2019, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourcePolicies",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShares",
        "ram:ListPendingInvitationResources",
        "ram:ListPrincipals",
        "ram:ListResources",
        "ram:RejectResourceShareInvitation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSResourceAccessManagerServiceRolePolicy

Descrição: Política contendo acesso do Read-only AWS Resource Access Manager à estrutura das organizações dos clientes. Ela também contém permissões do IAM para excluir a função.

`AWSResourceAccessManagerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Hora da criação: 14 de novembro de 2018, 19:28 UTC
- Hora da edição: 14 de novembro de 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDeletionOfServiceLinkedRoleForResourceAccessManager",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ram.amazonaws.com/*"
```

```
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSResourceExplorerFullAccess

Descrição: Essa política concede permissões administrativas para acessar os recursos do Resource Explorer e concede permissões somente para leitura a outros AWS serviços para oferecer suporte a esse acesso.

`AWSResourceExplorerFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSResourceExplorerFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 07 de novembro de 2022, 20:01 UTC
- Hora da edição: 14 de novembro de 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerConsoleFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceExplorerSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSResourceExplorerOrganizationsAccess

Descrição: Essa política concede permissões administrativas ao Resource Explorer e concede permissões somente para leitura a outros AWS serviços para oferecer suporte a esse acesso. O administrador da AWS organização precisa dessas permissões para configurar e gerenciar a pesquisa em várias contas no console.

`AWSResourceExplorerOrganizationsAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSResourceExplorerOrganizationsAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de novembro de 2023, 17:01 UTC
- Hora da edição: 14 de novembro de 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
```

```
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceExplorerGetSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer"
    },
    {
      "Sid" : "ResourceExplorerCreateSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationsAdministratorAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
```

```
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSResourceExplorerReadOnlyAccess

Descrição: Essa política concede permissões somente para leitura para pesquisar e visualizar recursos do Resource Explorer e concede permissões somente para leitura a outros AWS serviços para oferecer suporte a esse acesso.

`AWSResourceExplorerReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSResourceExplorerReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 07 de novembro de 2022, 19:56 UTC
- Hora da edição: 14 de novembro de 2023, 16:43 UTC

- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Get*",
        "resource-explorer-2:List*",
        "resource-explorer-2:Search",
        "resource-explorer-2:BatchGetView",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSResourceExplorerServiceRolePolicy

Descrição: permite que o Resource Explorer visualize recursos e CloudTrail eventos em seu nome para indexar seus recursos para pesquisa.

`AWSResourceExplorerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 25 de outubro de 2022, 20:35 UTC
- Horário editado: 01 de outubro de 2026, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

Versão da política

Versão da política: v56 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerAndOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:UpdateIndexType",
```

```
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:DeleteIndex",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudTrailEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/resource-
explorer-2/*"
    },
    {
      "Sid" : "ApiGatewayAccess",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/routes/*",
```

```
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*"
      ]
    },
    {
      "Sid" : "ResourceInventoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ValidatePolicy",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:ListEnvironments",
        "amplify:GetDomainAssociation",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListTagsForResource",
        "amplifyuibuilder:GetComponent",
        "amplifyuibuilder:ListComponents",
        "amplifyuibuilder:ListForms",
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
```

```
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "app-integrations:GetApplication",
        "app-integrations:GetDataIntegration",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListApplications",
        "app-integrations:ListDataIntegrations",
        "app-integrations:ListEventIntegrations",
        "app-integrations:ListTagsForResource",
        "appconfig:GetExtension",
        "appconfig:ListApplications",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appflow:DescribeConnector",
        "appflow:DescribeFlow",
        "appflow:ListConnectors",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScheduledActions",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource",
        "applicationinsights:DescribeApplication",
        "applicationinsights:DescribeComponent",
        "applicationinsights:DescribeLogPattern",
        "applicationinsights:ListApplications",
        "applicationinsights:ListComponents",
        "applicationinsights:ListLogPatternSets",
        "applicationinsights:ListLogPatterns",
        "applicationinsights:ListTagsForResource",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeAutoScalingConfiguration",
```

```
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListServices",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:DescribeAppBlockBuilders",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeApplications",
        "appstream:DescribeFleets",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appstream:ListAssociatedFleets",
        "appstream:ListAssociatedStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApi",
        "appsync:GetApiAssociation",
        "appsync:GetApiCache",
        "appsync:GetChannelNamespace",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetGraphqlApi",
        "appsync:GetResolver",
        "appsync:GetSourceApiAssociation",
        "appsync:ListApis",
        "appsync:ListChannelNamespaces",
        "appsync:ListDataSources",
        "appsync:ListDomainNames",
        "appsync:ListGraphqlApis",
        "appsync:ListResolvers",
        "appsync:ListSourceApiAssociations",
        "appsync:ListTagsForResource",
        "appsync:ListTypes",
        "apptest:GetTestCase",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "aps:DescribeAnomalyDetector",
        "aps:DescribeQueryLoggingConfiguration",
        "aps:DescribeResourcePolicy",
        "aps:DescribeRuleGroupsNamespace",
```

```
        "aps:DescribeScraper",
        "aps:DescribeScraperLoggingConfiguration",
        "aps:DescribeWorkspaceConfiguration",
        "aps:ListAnomalyDetectors",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "arc-region-switch:GetPlan",
        "arc-region-switch:ListPlans",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListTagsForResource",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:ListManagedResources",
        "athena:GetCapacityAssignmentConfiguration",
        "athena:GetCapacityReservation",
        "athena:ListCapacityReservations",
        "athena:ListDataCatalogs",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetControl",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessments",
        "auditmanager:ListControls",
        "auditmanager:ListTagsForResource",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "b2bi:GetCapability",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:ListCapabilities",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "b2bi:ListTagsForResource",
        "backup-gateway:GetHypervisor",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:ListBackupPlans",
```

```
        "backup:ListBackupVaults",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListRestoreTestingPlans",
        "backup:ListRestoreTestingSelections",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeConsumableResource",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobQueues",
        "batch:DescribeQuotaShare",
        "batch:DescribeServiceEnvironments",
        "batch:ListConsumableResources",
        "batch:ListQuotaShares",
        "batch:ListSchedulingPolicies",
        "bcm-dashboards:GetDashboard",
        "bcm-dashboards:ListDashboards",
        "bcm-dashboards:ListTagsForResource",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:ListExports",
        "bcm-data-exports:ListTagsForResource",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetConfigurationBundle",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPaymentConnector",
        "bedrock-agentcore:GetPaymentManager",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetPolicyEngineSummary",
        "bedrock-agentcore:GetPolicyGeneration",
        "bedrock-agentcore:GetPolicySummary",
        "bedrock-agentcore:GetResourcePolicy",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
```

```
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListConfigurationBundles",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:ListPaymentConnectors",
        "bedrock-agentcore:ListPaymentManagers",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngineSummaries",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListPolicyGenerations",
        "bedrock-agentcore:ListPolicySummaries",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock:GetAgentAlias",
        "bedrock:GetAutomatedReasoningPolicy",
        "bedrock:GetBlueprint",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataSource",
        "bedrock:GetEvaluationJob",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetInferenceProfile",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgents",
        "bedrock:ListAutomatedReasoningPolicies",
        "bedrock:ListBlueprints",
        "bedrock:ListCustomModels",
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListDataSources",
        "bedrock:ListEnforcedGuardrailsConfiguration",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlowVersions",
        "bedrock:ListFlows",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
```

```
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "billing:GetBillingView",
        "billing:ListBillingViews",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:ViewBudget",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:GetMicrosoftTeamsChannelConfiguration",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chime:DescribeAppInstance",
        "chime:ListAppInstanceBots",
        "chime:ListAppInstanceUsers",
        "chime:ListAppInstances",
        "chime:ListMediaInsightsPipelineConfigurations",
        "chime:ListMediaPipelineKinesisVideoStreamPools",
        "chime:ListMediaPipelines",
        "chime:ListSipMediaApplications",
        "chime:ListTagsForResource",
        "chime:ListVoiceConnectors",
        "cleanrooms-ml:GetConfiguredModelAlgorithm",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetConfiguredTableAssociationAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
```

```
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListTagsForResource",
        "cloud9:ListEnvironments",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribePublisher",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeType",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSets",
        "cloudformation:ListStacks",
        "cloudformation:ListTypes",
        "cloudfront:DescribeFunction",
        "cloudfront:DescribeKeyValueStore",
        "cloudfront:GetAnycastIpList",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetConnectionGroup",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistributionTenant",
        "cloudfront:GetKeyGroup",
        "cloudfront:GetMonitoringSubscription",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetVpcOrigin",
        "cloudfront:ListAnycastIpLists",
        "cloudfront:ListCachePolicies",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListConnectionGroups",
        "cloudfront:ListContinuousDeploymentPolicies",
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListDistributions",
        "cloudfront:ListFieldLevelEncryptionConfigs",
        "cloudfront:ListFieldLevelEncryptionProfiles",
```

```
        "cloudfront:ListFunctions",
        "cloudfront:ListKeyGroups",
        "cloudfront:ListKeyValueStores",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudfront:ListVpcOrigins",
        "cloudhsm:DescribeClusters",
        "cloudtrail:GetDashboard",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:ListChannels",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeInsightRules",
        "cloudwatch:ListAlarmMuteRules",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListManagedInsightRules",
        "cloudwatch:ListMetricStreams",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackageGroup",
        "codeartifact:DescribeRepository",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListAllowedRepositoriesForGroup",
        "codeartifact:ListDomains",
        "codeartifact:ListPackageGroups",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetFleets",
        "codebuild:ListFleets",
        "codebuild:ListProjects",
        "codecommit:ListRepositories",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections:ListHosts",
        "codedeploy:GetApplication",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:ListApplications",
```

```
        "codedeploy:ListDeploymentConfigs",
        "codedeploy:ListTagsForResource",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-profiler:ListTagsForResource",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:ListTagsForResource",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "codepipeline:ListWebhooks",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:ListConnections",
        "codestar-connections:ListHosts",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListSyncConfigurations",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:AdminGetUser",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeManagedLoginBranding",
        "cognito-idp:DescribeTerms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListTerms",
        "cognito-idp:ListUserPools",
        "comprehend:DescribeDocumentClassifier",
        "comprehend:DescribeFlywheel",
        "comprehend:DescribeResourcePolicy",
        "comprehend:ListDocumentClassifiers",
        "comprehend:ListEntityRecognizers",
        "comprehend:ListFlywheels",
        "comprehend:ListTagsForResource",
        "config:DescribeConfigRules",
        "config:DescribeConformancePacks",
        "config:DescribeOrganizationConformancePacks",
        "config:GetStoredQuery",
```

```
        "config:ListStoredQueries",
        "config:ListTagsForResource",
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:ListCampaigns",
        "connect:DescribeAgentStatus",
        "connect:DescribeEmailAddress",
        "connect:DescribeEvaluationForm",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUser",
        "connect:DescribeUserHierarchyGroup",
        "connect:DescribeUserHierarchyStructure",
        "connect:DescribeView",
        "connect:GetTaskTemplate",
        "connect:ListAgentStatuses",
        "connect:ListApprovedOrigins",
        "connect:ListBots",
        "connect:ListEvaluationFormVersions",
        "connect:ListEvaluationForms",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstanceStorageConfigs",
        "connect:ListInstances",
        "connect:ListIntegrationAssociations",
        "connect:ListLambdaFunctions",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPredefinedAttributes",
        "connect:ListPrompts",
        "connect:ListQueueEmailAddresses",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileManualAssignmentQueues",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
```

```
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfileFlowModules",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListTrafficDistributionGroups",
        "connect:ListUserHierarchyGroups",
        "connect:ListUsers",
        "connect:ListViewVersions",
        "connect:ListViews",
        "connect:SearchAvailablePhoneNumbers",
        "controltower:GetEnabledBaseline",
        "controltower:GetEnabledControl",
        "controltower:GetLandingZone",
        "controltower:ListEnabledBaselines",
        "controltower:ListEnabledControls",
        "controltower:ListLandingZones",
        "controltower:ListTagsForResource",
        "cur:DescribeReportDefinitions",
        "cur:ListTagsForResource",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:ListDataSets",
        "datapipeline:ListPipelines",
        "datasync:DescribeLocationAzureBlob",
        "datasync:DescribeLocationFsxOntap",
        "datasync:DescribeLocationFsxOpenZfs",
        "datasync:ListLocations",
        "datasync:ListTasks",
        "datazone:GetDataSource",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetGroupProfile",
```

```
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListDomains",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListSubscriptionTargets",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "dax:DescribeClusters",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetQueueLimitAssociation",
        "deadline:GetStorageProfile",
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListLicenseEndpoints",
        "deadline:ListMonitors",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListQueueLimitAssociations",
        "deadline:ListQueues",
        "deadline:ListStorageProfiles",
        "deadline:ListTagsForResource",
        "detective:GetMembers",
        "detective:ListGraphs",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTestGridProjects",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:ListNotificationChannels",
```

```
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualInterfaces",
        "dlm:GetLifecyclePolicies",
        "dms:DescribeCertificates",
        "dms:DescribeDataMigrations",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationConfigs",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTasks",
        "dms:ListDataProviders",
        "dms:ListInstanceProfiles",
        "dms:ListMigrationProjects",
        "dms:ListTagsForResource",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListTagsForResource",
        "ds:DescribeDirectories",
        "dsql:GetCluster",
        "dsql:GetClusterPolicy",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:ListTables",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAwsNetworkPerformanceMetricSubscriptions",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImages",
        "ec2:DescribeHostReservations",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeImportImageTasks",
```

```
        "ec2:DescribeInstanceConnectEndpoints",
        "ec2:DescribeInstanceEventWindows",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpamResourceDiscoveries",
        "ec2:DescribeIpamResourceDiscoveryAssociations",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeIpams",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayMeteringPolicies",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
```

```
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstanceLoggingConfigurations",
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcEncryptionControls",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetRouteServerAssociations",
        "ec2:GetRouteServerPropagations",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetSubnetCidrReservations",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeRepositories",
        "ecr:DescribeRepositories",
        "ecr:DescribeRepositoryCreationTemplates",
        "ecr:GetRegistryScanningConfiguration",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeServices",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
```

```
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeCapability",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListClusters",
        "eks:ListEksAnywhereSubscriptions",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeReservedCacheNodes",
        "elasticache:DescribeServerlessCaches",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeListenerAttributes",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTrustStoreRevocations",
        "elasticloadbalancing:DescribeTrustStores",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:GetAutoTerminationPolicy",
```

```
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListSteps",
        "elemental-inference:GetFeed",
        "elemental-inference:ListFeeds",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:ListJobRuns",
        "emr-containers:ListJobTemplates",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListSecurityConfigurations",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:ListApplications",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetIdNamespace",
        "entityresolution:GetMatchingWorkflow",
        "entityresolution:GetPolicy",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "entityresolution:ListIdNamespaces",
        "entityresolution:ListMatchingWorkflows",
        "entityresolution:ListSchemaMappings",
        "entityresolution:ListTagsForResource",
        "es:GetApplication",
        "es:ListApplications",
        "es:ListDomainNames",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "finspace:ListEnvironments",
        "firehose:ListDeliveryStreams",
        "fis:GetTargetAccountConfiguration",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fis:ListTargetAccountConfigurations",
        "fms:ListPolicies",
```

```
        "fms:ListProtocolsLists",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasetImportJobs",
        "forecast:ListDatasets",
        "forecast:ListForecastExportJobs",
        "forecast:ListForecasts",
        "forecast:ListPredictorBacktestExportJobs",
        "forecast:ListPredictors",
        "frauddetector:GetDetectors",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetVariables",
        "fsx:DescribeBackups",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "gamelift:DescribeContainerFleet",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeScalingPolicies",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListContainerFleets",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "gameliftstreams:GetApplication",
        "gameliftstreams:GetStreamGroup",
        "gameliftstreams:ListApplications",
        "gameliftstreams:ListStreamGroups",
        "gameliftstreams:ListTagsForResource",
        "geo:DescribeKey",
        "geo:ListKeys",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListTrackers",
        "glacier:ListVaults",
        "globalaccelerator:DescribeCrossAccountAttachment",
```

```
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCrossAccountAttachments",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "glue:GetBlueprint",
        "glue:GetCrawlers",
        "glue:GetDatabases",
        "glue:GetJobs",
        "glue:GetRegistry",
        "glue:GetSchemaVersion",
        "glue:GetSession",
        "glue:GetTables",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetTriggers",
        "glue:ListDataQualityRulesets",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListSchemaVersions",
        "glue:ListSessions",
        "glue:ListTriggers",
        "glue:querySchemaVersionMetadata",
        "grafana:ListWorkspaces",
        "greengrass:GetDeployment",
        "greengrass:ListComponentVersions",
        "greengrass:ListComponents",
        "greengrass:ListConnectorDefinitions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeployments",
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroups",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListResourceDefinitions",
        "greengrass:ListSubscriptionDefinitions",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetThreatEntitySet",
        "guardduty:GetTrustedEntitySet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListIPSets",
```

```
        "guardduty:ListMalwareProtectionPlans",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListThreatEntitySets",
        "guardduty:ListThreatIntelSets",
        "guardduty:ListTrustedEntitySets",
        "healthlake:GetDataTransformationProfile",
        "healthlake:ListFHIRDatastores",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListInstanceProfiles",
        "iam:ListMFADevices",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
        "imagebuilder:ListWorkflowBuildVersions",
```

```
        "imagebuilder:ListWorkflows",
        "inspector2:GetCodeSecurityScanConfiguration",
        "inspector2:ListCisScanConfigurations",
        "inspector2:ListCodeSecurityScanConfigurations",
        "inspector2:ListFilters",
        "inspector2:ListTagsForResource",
        "inspector:ListAssessmentTemplates",
        "internetmonitor:ListTagsForResource",
        "iot:DescribeCertificateProvider",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetCommand",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetV2LoggingOptions",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificateProviders",
        "iot:ListCertificates",
        "iot:ListCommands",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListJobs",
        "iot:ListMitigationActions",
        "iot:ListOTAUpdates",
        "iot:ListPackageVersions",
        "iot:ListPackages",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListStreams",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListThings",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListTunnels",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
```

```
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetStateTemplate",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListStateTemplates",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeComputationModel",
        "iotsitewise:DescribeDataset",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListComputationModels",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjects",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetPartnerAccount",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListDevicesForWirelessDeviceImportTask",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
```

```
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "iotwireless:ListWirelessGateways",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetStage",
        "ivs:GetStorageConfiguration",
        "ivs:ListChannels",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:DescribeReplicator",
        "kafka:ListClusters",
        "kafka:ListConfigurations",
        "kafka:ListReplicators",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra-ranking:ListRescoreExecutionPlans",
        "kendra:ListAccessControlConfigurations",
        "kendra:ListDataSources",
        "kendra:ListExperiences",
        "kendra:ListFaqs",
        "kendra:ListFeaturedResultsSets",
        "kendra:ListIndices",
        "kendra:ListQuerySuggestionsBlockLists",
        "kendra:ListThesauri",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kms:ListKeys",
```

```
        "lakeformation:ListDataCellsFilter",
        "lambda:ListCapacityProviders",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "lambda:ListLayerVersions",
        "lambda:ListLayers",
        "lambda:ListVersionsByFunction",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListTagsForResource",
        "lex:ListBotAliases",
        "lex:ListBots",
        "license-manager:ListDistributedGrants",
        "license-manager:ListTagsForResource",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDisks",
        "lightsail:GetInstanceSnapshot",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:ListTagsForResource",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutvision:ListProjects",
        "m2:ListEnvironments",
        "macie2:ListAllowLists",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindingsFilters",
        "macie2:ListMembers",
        "managedblockchain:ListAccessors",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGateways",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:ListChannels",
        "mediapackage:ListOriginEndpoints",
        "mediastore:ListContainers",
        "mediatailor:ListChannels",
```

```
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "memorydb:DescribeACLs",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeSnapshots",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTemplates",
        "mq:ListBrokers",
        "mq:ListConfigurations",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetDevices",
        "networkmanager:GetLinks",
        "networkmanager:ListAttachments",
        "networkmanager:ListCoreNetworks",
        "oam:ListSinks",
        "omics:ListReferenceStores",
        "omics:ListRunGroups",
        "omics:ListWorkflows",
        "organizations:DescribeResourcePolicy",
        "organizations:ListPolicies",
        "outposts:ListSites",
        "panorama:ListDevices",
        "panorama:ListPackages",
        "partnercentral:ListBenefitApplications",
        "partnercentral:ListEngagementInvitations",
        "partnercentral:ListEngagements",
        "partnercentral:ListOpportunities",
        "partnercentral:ListResourceSnapshotJobs",
        "partnercentral:ListResourceSnapshots",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "pipes:ListPipes",
```

```
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentTemplates",
        "proton:ListServiceTemplates",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListLedgers",
        "quicksight:DescribeAccountSubscription",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListFolders",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "ram:GetResourceShares",
        "ram:ListPermissions",
        "rbin:ListRules",
        "rbin:ListTagsForResource",
        "rds:DescribeBlueGreenDeployments",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeReservedDBInstances",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeHsmClientCertificates",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeSnapshotSchedules",
```

```
        "redshift:DescribeUsageLimits",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "rekognition:DescribeProjects",
        "rekognition:ListCollections",
        "resiliencehub:ListAppAssessments",
        "resiliencehub:ListApps",
        "resiliencehub:ListResiliencyPolicies",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListViews",
        "resource-groups:ListGroups",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53domains:ListDomains",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRules",
        "rum:ListAppMonitors",
        "s3:GetBucketLocation",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3express:ListAllMyDirectoryBuckets",
        "s3vectors:ListIndexes",
        "s3vectors:ListVectorBuckets",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:ListActions",
```

```
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListClusters",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListContexts",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHubContents",
        "sagemaker:ListHubs",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPartnerApps",
        "sagemaker:ListPipelines",
        "sagemaker:ListProjects",
        "sagemaker:ListSpaces",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "scheduler:ListScheduleGroups",
        "schemas:ListDiscoverers",
        "secretsmanager:ListSecrets",
        "servicecatalog:ListApplications",
```

```
        "servicecatalog:ListAttributeGroups",
        "servicediscovery:ListServices",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailIdentities",
        "ses:ListEmailTemplates",
        "shield:ListProtectionGroups",
        "shield:ListProtections",
        "signer:ListSigningProfiles",
        "sns:ListTopics",
        "sqs:ListQueues",
        "ssm-incidents:ListResponsePlans",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindowTargets",
        "ssm:DescribeMaintenanceWindowTasks",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
        "ssm:DescribeSessions",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "states:ListActivities",
        "states:ListStateMachines",
        "storagegateway:ListFileShares",
        "storagegateway:ListGateways",
        "swf:ListDomains",
        "synthetics:DescribeCanaries",
        "synthetics:ListGroups",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "verifiedpermissions:ListPolicyStores",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
```

```
        "vpc-lattice:ListTargetGroups",
        "wafv2:ListIPSets",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListRuleGroups",
        "wafv2:ListWebACLs",
        "wellarchitected:ListWorkloads",
        "wisdom:ListAssistantAssociations",
        "wisdom:ListAssistants",
        "wisdom:ListContents",
        "wisdom:ListKnowledgeBases",
        "workspaces-web:ListPortals",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaces",
        "xray:GetSamplingRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsForReadGetResources",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListTagsForResource",
        "account-access:GetEntitlement",
        "account-access:ListEntitlements",
        "account:GetAlternateContact",
        "airflow:GetEnvironment",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListThemes",
        "app-integrations:ListEventIntegrationAssociations",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExperimentDefinition",
        "appconfig:GetExtensionAssociation",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListExperimentDefinitions",
```

```
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "application-autoscaling:DescribeScalingPolicies",
        "apprunner:ListTagsForResource",
        "appstream:DescribeDirectoryConfigs",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeWorkspace",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "b2bi:GetTransformer",
        "b2bi:ListTransformers",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetTieringConfiguration",
        "backup:ListBackupSelections",
        "backup:ListFrameworks",
        "backup:ListTags",
        "backup:ListTieringConfigurations",
        "batch:DescribeSchedulingPolicies",
        "batch:ListTagsForResource",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetBrowserProfile",
        "bedrock-agentcore:GetPaymentCredentialProvider",
        "bedrock-agentcore:GetPolicyGenerationSummary",
```

```
        "bedrock-agentcore:ListBrowserProfiles",
        "bedrock-agentcore:ListPaymentCredentialProviders",
        "bedrock-agentcore:ListPolicyGenerationSummaries",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetFlowAlias",
        "bedrock:GetGuardrail",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetPromptRouter",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "braket:ListTagsForResource",
        "braket:SearchSpendingLimits",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForBudget",
        "cases:BatchGetCaseRule",
        "cases:BatchGetField",
        "cases:GetDomain",
        "cases:GetLayout",
        "cases:GetTemplate",
        "cases:ListCaseRules",
        "cases:ListDomains",
        "cases:ListFields",
        "cases:ListLayouts",
        "cases:ListTemplates",
        "cassandra:Select",
        "chime:DescribeAppInstanceBot",
        "chime:DescribeAppInstanceUser",
        "chime:DescribeChannelFlow",
        "chime:ListChannelFlows",
        "cleanrooms-ml:ListConfiguredModelAlgorithms",
        "cleanrooms:GetAnalysisTemplate",
```

```
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:ListMembers",
        "cleanrooms:ListTagsForResource",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:DescribeChangeSet",
        "cloudformation:GetResource",
        "cloudformation:ListChangeSets",
        "cloudformation:ListStackResources",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetFunction",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetChannel",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetAlarmMuteRule",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListTagsForResource",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListReportGroups",
        "codebuild:ListSourceCredentials",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListTagsForResource",
        "codeconnections:ListTagsForResource",
        "codedeploy:GetDeployment",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:ListDeploymentGroups",
        "codedeploy:ListDeployments",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
```

```
        "codestar-connections:ListTagsForResource",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "config:DescribeAggregationAuthorizations",
        "connect:DescribeDataTable",
        "connect:DescribeHoursOfOperation",
        "connect:DescribeMetric",
        "connect:DescribeNotification",
        "connect:DescribeQueue",
        "connect:DescribeWorkspace",
        "connect:ListDataTables",
        "connect:ListHoursOfOperationOverrides",
        "connect:ListInstances",
        "connect:ListMetrics",
        "connect:ListNotifications",
        "connect:ListQuickConnects",
        "connect:ListSecurityProfileAIAgents",
        "connect:ListUserProficiencies",
        "connect:ListUsers",
        "connect:ListWorkspaceMedia",
        "connect:ListWorkspacePages",
        "connect:ListWorkspaces",
        "connect:SearchWorkspaceAssociations",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipeVersions",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
```

```
        "dataexchange:GetRevision",
        "dataexchange:ListTagsForResource",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "deadline:GetBudget",
        "deadline:GetJob",
        "deadline:ListBudgets",
        "deadline:ListJobs",
        "deadline:SearchJobs",
        "detective:DescribeOrganizationConfiguration",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListTagsForResource",
        "devops-guru:GetResourceCollection",
        "directconnect:DescribeLags",
        "dlm:GetLifecyclePolicy",
        "dlm:ListTagsForResource",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeGlobalTableSettings",
```

```
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeClientVpnTargetNetworks",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeRouteServerEndpoints",
        "ec2:DescribeRouteServerPeers",
        "ec2:DescribeRouteServers",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeVolumeAttribute",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeClusters",
        "ecs:DescribeExpressGatewayService",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "eks:DescribeCluster",
        "eks:ListCapabilities",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheSecurityGroups",
```

```
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:ListTagsForResource",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:DescribeCapacityReservation",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "elemental-inference:ListTagsForResource",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListJobRuns",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainsForPackage",
        "es:ListTags",
        "es:ListVpcEndpointsForDomain",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
```

```
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperiment",
        "fis:GetExperimentTemplate",
        "fis:ListTagsForResource",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListTagsForResource",
        "frauddetector:GetListElements",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeS3AccessPointAttachments",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeContainerGroupDefinition",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListBuilds",
        "gamelift:ListContainerGroupDefinitions",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "gamelift:ValidateMatchmakingRuleSet",
        "geo:DescribeGeofenceCollection",
```

```
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeAcceleratorAttributes",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:DescribeIntegrations",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetDatabase",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetWorkflow",
        "glue:ListBlueprints",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListTagsForResource",
        "greengrass:DescribeComponent",
        "greengrass:ListTagsForResource",
```

```
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListFindings",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListTagsForResource",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListDataTransformationProfiles",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:ListAttachedRolePolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADeviceTags",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "imagebuilder:GetComponent",
```

```
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListMembers",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListMonitors",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:ListTagsForResource",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJob",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:GetPolicy",
        "iot:GetTopicRuleDestination",
        "iot:ListDomainConfigurations",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
```

```
        "iotfleetwise:ListTagsForResource",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListTagsForResource",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "ivs:GetComposition",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetRecordingConfiguration",
        "ivs:ListCompositions",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
        "kafka:ListClustersV2",
```

```
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListTagsForResource",
        "kendra-ranking:DescribeRescoreExecutionPlan",
        "kendra-ranking:ListTagsForResource",
        "kendra:DescribeIndex",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetResourcePolicy",
        "kinesis:ListStreamConsumers",
        "kinesis:ListTagsForResource",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListResourceTags",
        "lakeformation:DescribeLakeFormationIdentityCenterConfiguration",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionScalingConfig",
```

```
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListTags",
        "launchwizard:GetDeployment",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotLocales",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "lightsail:GetActiveNames",
        "lightsail:GetDisk",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetLoadBalancers",
        "lightsail:GetOperations",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDeliveries",
```

```
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeIndexPolicies",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetIntegration",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeMetricSet",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListTagsForResource",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
```

```
        "mediaconnect:DescribeGateway",
        "mediaconnect:GetRouterInput",
        "mediaconnect:GetRouterNetworkInterface",
        "mediaconnect:ListBridges",
        "mediaconnect:ListRouterInputs",
        "mediaconnect:ListRouterNetworkInterfaces",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListTagsForResource",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeNode",
        "medialive:DescribeSdiSource",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:ListChannelPlacementGroups",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListMultiplexPrograms",
        "medialive:ListMultiplexes",
        "medialive:ListNodes",
        "medialive:ListSdiSources",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:DescribeAsset",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListTagsForResource",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediatailor:DescribeChannel",
        "mediatailor:DescribeLiveSource",
        "mediatailor:DescribeSourceLocation",
```

```
        "mediatailor:DescribeVodSource",
        "mediatailor:GetChannelPolicy",
        "mediatailor:GetPlaybackConfiguration",
        "medical-imaging:GetDatastore",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListTagsForResource",
        "memorydb:DescribeParameters",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetEmailChannel",
        "mobiletargeting:GetEmailTemplate",
        "mobiletargeting:GetEventStream",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:GetSegment",
        "mobiletargeting:ListTagsForResource",
        "mpa:GetIdentitySource",
        "mpa:ListIdentitySources",
        "mpa:ListTagsForResource",
        "mq:DescribeBroker",
        "mq:DescribeConfiguration",
        "mq:ListTags",
        "neptune-graph:GetGraphSnapshot",
        "neptune-graph:GetPrivateGraphEndpoint",
        "neptune-graph:ListGraphSnapshots",
        "neptune-graph:ListPrivateGraphEndpoints",
        "neptune-graph:ListTagsForResource",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:DescribeVpcEndpointAssociation",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:ListVpcEndpointAssociations",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDirectConnectGatewayAttachment",
        "networkmanager:GetLinkAssociations",
```

```
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:ListTagsForResource",
        "notifications:GetEventRule",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications:ListOrganizationalUnits",
        "notifications:ListTagsForResource",
        "nova-act:GetWorkflowDefinition",
        "nova-act:ListWorkflowDefinitions",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListLinks",
        "oam:ListTagsForResource",
        "omics:GetAnnotationStore",
        "omics:GetConfiguration",
        "omics:GetReferenceStore",
        "omics:GetRun",
        "omics:GetRunCache",
        "omics:GetRunGroup",
        "omics:GetS3AccessPolicy",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:GetWorkflowVersion",
        "omics:ListAnnotationStores",
        "omics:ListConfigurations",
        "omics:ListRunCaches",
        "omics:ListRuns",
        "omics:ListSequenceStores",
        "omics:ListTagsForResource",
        "omics:ListVariantStores",
```

```
        "omics:ListWorkflowVersions",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "osis:GetPipeline",
        "osis:GetResourcePolicy",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "outposts:GetSite",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeDevice",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListTagsForResource",
        "partnercentral:GetBenefitApplication",
        "partnercentral:ListTagsForResource",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListChallengeMetadata",
        "pca-connector-scep:ListConnectors",
```

```
        "pca-connector-scep:ListTagsForResource",
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetImportJobs",
        "personalize:ListTagsForResource",
        "pipes:DescribePipe",
        "profile:GetCalculatedAttributeDefinition",
        "profile:GetDomain",
        "profile:GetEventStream",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListCalculatedAttributeDefinitions",
        "profile:ListDomains",
        "profile:ListEventStreams",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetPolicy",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:ListApplications",
        "qbusiness:ListDataSources",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeCustomPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
```

```
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeOAuthClientApplication",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:DescribeTopic",
        "quicksight:DescribeVPCConnection",
        "quicksight:ListAnalyses",
        "quicksight:ListCustomPermissions",
        "quicksight:ListDashboards",
        "quicksight:ListOAuthClientApplications",
        "quicksight:ListRefreshSchedules",
        "quicksight:ListTagsForResource",
        "quicksight:ListTopics",
        "quicksight:ListVPCConnections",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:ListPermissionAssociations",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeIntegrations",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
```

```
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterDbRevisions",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeDataShares",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListTagsForResource",
        "rekognition:DescribeCollection",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListTagsForResource",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
```

```
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53:GetChange",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListOutpostResolvers",
        "route53resolver:ListResolverConfigs",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverRuleAssociations",
```

```
        "route53resolver:ListTagsForResource",
        "rtbfabric:GetCertificateAssociation",
        "rtbfabric:GetInboundExternalLink",
        "rtbfabric:GetLink",
        "rtbfabric:GetLinkRoutingRule",
        "rtbfabric:GetOutboundExternalLink",
        "rtbfabric:GetRequesterGateway",
        "rtbfabric:GetResponderGateway",
        "rtbfabric:ListCertificateAssociations",
        "rtbfabric:ListLinkRoutingRules",
        "rtbfabric:ListLinks",
        "rtbfabric:ListRequesterGateways",
        "rtbfabric:ListResponderGateways",
        "rtbfabric:ListTagsForResource",
        "rum:GetAppMonitor",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
```

```
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListTagsForResource",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetInventoryConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:GetMetricsConfiguration",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListTagsForResource",
        "s3files:GetAccessPoint",
        "s3files:GetFileSystem",
        "s3files:GetFileSystemPolicy",
        "s3files:GetMountTarget",
        "s3files:GetSynchronizationConfiguration",
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems",
        "s3files:ListMountTargets",
        "s3files:ListTagsForResource",
```

```
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketMetricsConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:ListTableBuckets",
        "s3tables:ListTagsForResource",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:ListTagsForResource",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeClusterSchedulerConfig",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeComputeQuota",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHub",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeMlflowApp",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
```

```
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelCardExportJob",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribePartnerApp",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTrainingPlan",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListClusterSchedulerConfigs",
        "sagemaker:ListComputeQuotas",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListMlflowApps",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCardExportJobs",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListOptimizationJobs",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
```

```
        "sagemaker:ListTrainingPlans",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "sdb:GetAttributes",
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecretVersionIds",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetTargetDomains",
        "securityagent:GetApplication",
        "securityagent:ListApplications",
        "securityagent:ListPentests",
        "securityagent:ListTagsForResource",
        "securityagent:ListTargetDomains",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetAggregatorV2",
        "securityhub:GetAutomationRuleV2",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:ListAggregatorsV2",
        "securityhub:ListAutomationRulesV2",
        "securityhub:ListConfigurationPolicies",
        "securityhub:ListConfigurationPolicyAssociations",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:ListFindingAggregators",
        "securityhub:ListTagsForResource",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
```

```
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "servicecatalog:DescribePortfolio",
        "servicecatalog:DescribePortfolioShares",
        "servicecatalog:DescribeProductAsAdmin",
        "servicecatalog:DescribeProvisionedProduct",
        "servicecatalog:DescribeProvisioningArtifact",
        "servicecatalog:DescribeServiceAction",
        "servicecatalog:DescribeTagOption",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListPortfolios",
        "servicecatalog:ListProvisioningArtifacts",
        "servicecatalog:ListServiceActions",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:ListTagOptions",
        "servicecatalog:SearchProductsAsAdmin",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetAddonInstance",
        "ses:GetAddonSubscription",
        "ses:GetAddressList",
        "ses:GetArchive",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailIdentity",
        "ses:GetEmailTemplate",
        "ses:GetIngressPoint",
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:ListAddonInstances",
        "ses:ListAddonSubscriptions",
```

```
        "ses:ListAddressLists",
        "ses:ListArchives",
        "ses:ListIngressPoints",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListRelays",
        "ses:ListRuleSets",
        "ses:ListTagsForResource",
        "ses:ListTemplates",
        "ses:ListTrafficPolicies",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeProtectionGroup",
        "shield:DescribeSubscription",
        "shield:ListTagsForResource",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "simspaceweaver:DescribeSimulation",
        "simspaceweaver:ListSimulations",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeProtectConfigurations",
        "sms-voice:DescribeSenderIds",
        "sms-voice:GetProtectConfigurationCountryRuleSet",
        "sms-voice:GetResourcePolicy",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:GetRotation",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
```

```
        "ssm-contacts:ListRotations",
        "ssm-contacts:ListTagsForResource",
        "ssm-guiconnect:GetConnectionRecordingPreferences",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListTagsForResource",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:GetApplication",
        "ssm-sap:ListApplications",
        "ssm-sap:ListTagsForResource",
        "ssm:DescribeAssociation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribePatchBaselines",
        "ssm:GetAutomationExecution",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetMaintenanceWindow",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:GetServiceSetting",
        "ssm:ListTagsForResource",
        "sso:DescribeApplication",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:ListApplications",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineAlias",
        "states:ListStateMachineAliases",
        "states:ListStateMachineVersions",
        "states:ListTagsForResource",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
```

```
        "support:DescribeCases",
        "supportapp:ListSlackChannelConfigurations",
        "supportapp:ListSlackWorkspaceConfigurations",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "textract:GetAdapter",
        "textract:ListAdapters",
        "textract:ListTagsForResource",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeScheduledQuery",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListScheduledQueries",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transcribe:GetCallAnalyticsJob",
        "transcribe:GetVocabularyFilter",
        "transcribe:ListCallAnalyticsJobs",
        "transcribe:ListTagsForResource",
        "transcribe:ListVocabularyFilters",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWebApp",
        "transfer:DescribeWebAppCustomization",
        "transfer:DescribeWorkflow",
        "transfer:ListTagsForResource",
        "transfer:ListWebApps",
```

```
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicyTemplates",
        "verifiedpermissions:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListTargets",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetIPSet",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRegexPatternSet",
        "wafv2:GetRuleGroup",
        "wafv2:GetWebACL",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListTagsForResource",
        "wisdom:GetAIAgent",
        "wisdom:GetAIGuardrail",
        "wisdom:GetAIPrompt",
        "wisdom:GetAssistant",
        "wisdom:ListAIAgentVersions",
        "wisdom:ListAIAgents",
        "wisdom:ListAIGuardrails",
```

```
        "wisdom:ListAIGuardrailVersions",
        "wisdom:ListAIPrompts",
        "wisdom:ListAIPromptVersions",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListIpAccessSettings",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspacesPools",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetIndexingRules",
        "xray:GetTraceSegmentDestination",
        "xray:ListResourcePolicies",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSResourceGroupsReadOnlyAccess

Descrição: Essa é a política somente para leitura para grupos AWS de recursos

`AWSResourceGroupsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSResourceGroupsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 7 de março de 2018, 10:27 UTC
- Hora da edição: 05 de fevereiro de 2019, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "tag:Get*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeSnapshots",
        "elasticache:ListTagsForResource",
```

```
        "elasticbeanstalk:DescribeEnvironments",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListClusters",
        "glacier:ListVaults",
        "glacier:DescribeVault",
        "glacier:ListTagsForVault",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:ListTagsForStream",
        "opsworks:DescribeStacks",
        "opsworks:ListTags",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeTags",
        "route53domains:ListDomains",
        "route53:ListHealthChecks",
        "route53:GetHealthCheck",
        "route53:ListHostedZones",
        "route53:GetHostedZone",
        "route53:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListTagsForResource",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "ssm:ListDocuments"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSRevenueAttributionManagement

Descrição: Fornece o acesso necessário para atividades de gerenciamento de atribuição de receita.

`AWSRevenueAttributionManagement` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSRevenueAttributionManagement` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 30 de junho de 2026, 16:57 UTC
- Horário editado: 30 de junho de 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRevenueAttributionManagement`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RevenueAttributionCreation",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateRevenueAttribution"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "RevenueAttributionListing",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListRevenueAttributions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "RevenueAttributionManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetRevenueAttribution",
        "partnercentral:UpdateRevenueAttribution"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/revenue-attribution/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "TaggingAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/revenue-attribution/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSRoboMaker_FullAccess

Descrição: Fornece acesso total AWS RoboMaker por meio do Console de gerenciamento da AWS e SDK. Também fornece acesso selecionado a serviços relacionados (por exemplo, S3, IAM).

`AWSRoboMaker_FullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSRoboMaker_FullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário da criação: 10 de setembro de 2020, 18:34 UTC
- Hora da edição: 16 de setembro de 2021, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "robomaker:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecr:BatchGetImage",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecr-public:DescribeImages",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSRoboMakerReadOnlyAccess

Descrição: Fornece acesso somente para leitura AWS RoboMaker por meio do Console de gerenciamento da AWS e SDK

`AWSRoboMakerReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSRoboMakerReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de novembro de 2018, 5:30 UTC
- Hora da edição: 28 de agosto de 2020, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSRoboMakerServicePolicy

Descrição: política RoboMaker de serviço

`AWSRoboMakerServicePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 26 de novembro de 2018, 6:30 UTC
- Hora da edição: 11 de novembro de 2021, 22:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetAssociatedRole",
        "lambda:CreateFunction",
        "robomaker:CreateSimulationJob",
        "robomaker:CancelSimulationJob"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "robomaker:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:robomaker:*:*:simulation-job/*"
    },
    {
      "Action" : [
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration",
        "lambda:DeleteFunction",
        "lambda:ListVersionsByFunction",
        "lambda:GetAlias",
        "lambda:UpdateAlias",
        "lambda:CreateAlias",
```

```
        "lambda:DeleteAlias"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:lambda:*:*:function:aws-robomaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "robomaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSRoboMakerServiceRolePolicy

Descrição: política RoboMaker de serviço

`AWSRoboMakerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSRoboMakerServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de novembro de 2018, 5:33 UTC

- Hora da edição: 26 de novembro de 2018, 5:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetAssociatedRole",
        "lambda:CreateFunction"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "lambda:UpdateFunctionCode",
```

```
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:lambda:*:*:function:aws-robomaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSRolesAnywhereFullAccess

Descrição: fornece todas as permissões aos recursos do IAM Roles Anywhere, incluindo, mas não se limitando a: CreateProfile, DeleteTrustAnchor, DisableCrl,. ResetNotificationSettings

`AWSRolesAnywhereFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSRolesAnywhereFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Horário de criação: 16 de julho de 2025, 14:52 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRolesAnywhereFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustAnchors",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTrustAnchors",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:CreateTrustAnchor",
        "rolesanywhere:DeleteTrustAnchor",
        "rolesanywhere:DisableTrustAnchor",
        "rolesanywhere:EnableTrustAnchor",
        "rolesanywhere:UpdateTrustAnchor"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:trust-anchor/*"
      ]
    },
    {
      "Sid" : "Profiles",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListProfiles",
        "rolesanywhere:GetProfile",
        "rolesanywhere:CreateProfile",
        "rolesanywhere:DeleteProfile",
```

```
        "rolesanywhere:DisableProfile",
        "rolesanywhere:EnableProfile",
        "rolesanywhere:UpdateProfile"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:profile/*"
      ]
    },
    {
      "Sid" : "CRLs",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListCrls",
        "rolesanywhere:GetCrl",
        "rolesanywhere:DeleteCrl",
        "rolesanywhere:DisableCrl",
        "rolesanywhere:EnableCrl",
        "rolesanywhere:ImportCrl",
        "rolesanywhere:UpdateCrl"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:crl/*"
      ]
    },
    {
      "Sid" : "Subjects",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListSubjects",
        "rolesanywhere:GetSubject"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:subject/*"
      ]
    },
    {
      "Sid" : "OtherRolesAnywherePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:PutAttributeMapping",
        "rolesanywhere:DeleteAttributeMapping",
        "rolesanywhere:ResetNotificationSettings",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:TagResource",
```

```
        "rolesanywhere:UntagResource",
        "rolesanywhere:PutNotificationSettings"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToRolesAnywhere",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "rolesanywhere.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateRolesAnywhereServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "rolesanywhere.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSRolesAnywhereReadOnly

Descrição: fornece permissões somente de leitura para os recursos do IAM Roles Anywhere, incluindo, mas não se limitando a: GetTrustAnchor, ListProfiles, getCRL. Não haverá outras permissões para outros serviços incluídos nesta política.

`AWSRolesAnywhereReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSRolesAnywhereReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 16 de julho de 2025, 15:07 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRolesAnywhereReadOnly`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Profiles",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListProfiles",
        "rolesanywhere:GetProfile"
      ],
      "Resource" : [
```

```
        "arn:aws:rolesanywhere:*:*:profile/*"
      ]
    },
    {
      "Sid" : "CRLs",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListCrls",
        "rolesanywhere:GetCrl"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:crl/*"
      ]
    },
    {
      "Sid" : "Subjects",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListSubjects",
        "rolesanywhere:GetSubject"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:subject/*"
      ]
    },
    {
      "Sid" : "TrustAnchors",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTrustAnchors",
        "rolesanywhere:GetTrustAnchor"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:trust-anchor/*"
      ]
    },
    {
      "Sid" : "Tags",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTagsForResource"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSRolesAnywhereServicePolicy

Descrição: permite que o IAM Roles Anywhere publique service/usage métricas CloudWatch e verifique o status das autoridades de certificação privadas em seu nome.

`AWSRolesAnywhereServicePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 05 de julho de 2022, 15:26 UTC
- Hora da edição: 05 de julho de 2022, 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/RolesAnywhere",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSS3OnOutpostsServiceRolePolicy

Descrição: permite que o serviço Amazon S3 no Outposts gerencie recursos de rede do EC2 em seu nome.

`AWSS3OnOutpostsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 03 de outubro de 2023, 20:32 UTC
- Hora da edição: 03 de outubro de 2023, 20:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:DescribeAddresses",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations"
      ],
      "Resource" : "*",
      "Sid" : "DescribeVpcResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Sid" : "CreateNetworkInterface"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "S3 On Outposts"
        }
      },
      "Sid" : "CreateTagsForCreateNetworkInterface"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:ipv4pool-ec2/*"
      ],
```

```
      "Sid" : "AllocateIpAddress"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "S3 On Outposts"
        }
      },
      "Sid" : "CreateTagsForAllocateIpAddress"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:AssociateAddress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "S3 On Outposts"
        }
      },
      "Sid" : "ReleaseVpcResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "AllocateAddress"
          ],
          "aws:RequestTag/CreatedBy" : [
            "S3 On Outposts"
          ]
        }
      },
      "Sid" : "CreateTags"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSavingsPlansFullAccess

Descrição: fornece acesso total ao serviço Savings Plans

`AWSSavingsPlansFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSavingsPlansFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de novembro de 2019, 22:45 UTC
- Hora da edição: 06 de novembro de 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "savingsplans:*",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSavingsPlansReadOnlyAccess

Descrição: fornece acesso somente leitura ao serviço Savings Plans

`AWSSavingsPlansReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSavingsPlansReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de novembro de 2019, 22:45 UTC
- Hora da edição: 06 de novembro de 2019, 22:45 UTC

- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "savingsplans:Describe*",
        "savingsplans:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSDMPServiceRolePolicy

Descrição: Permita que o SDMP crie e gerencie recursos em nome do cliente.

`AWSSDMPServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 24 de julho de 2026, 20:57 UTC
- Horário editado: 10 de agosto de 2026, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSDMPServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetServiceLinkedChannel",
        "cloudtrail:UpdateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/sdmp/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "AllowListOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels",
        "iam:ListPolicies",
        "iam:ListPolicyTags",
        "iam:ListRoles",
        "account:ListRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateRoleWithConditions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SDMP-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/AWSDenyAll"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:ResourceTag/CreatedBy" : "arn:aws:iam::*:role/SDMPServiceRole*"
        }
      }
    },
    {
      "Sid" : "AllowSDMPRoleTagging",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : "arn:aws:iam::*:role/SDMP-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "CreatedBy"
```

```
        ]
      }
    }
  },
  {
    "Sid" : "AttachAWSDenyAll",
    "Effect" : "Allow",
    "Action" : "iam:AttachRolePolicy",
    "Resource" : "arn:aws:iam::*:role/SDMP-*",
    "Condition" : {
      "ArnEquals" : {
        "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSDenyAll"
      },
      "StringLike" : {
        "aws:ResourceTag/CreatedBy" : "arn:aws:iam::*:role/SDMPServiceRole*"
      },
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "ReadSDMPRoles",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole",
      "iam:GetRolePolicy",
      "iam:ListRoleTags",
      "iam:ListRolePolicies",
      "iam:ListAttachedRolePolicies"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/SDMP-*",
      "arn:aws:iam::*:role/SDMPServiceRole*",
      "arn:aws:iam::*:role/aws-service-role/sdmp.amazonaws.com/AWSServiceRoleForSDMP"
    ]
  },
  {
    "Sid" : "ReadSDMPPolicies",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetPolicy",
      "iam:GetPolicyVersion",
      "iam:ListPolicyVersions"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/SDMP*"
      ]
    },
    {
      "Sid" : "AllowSecurityServiceVerification",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ListDetectors",
        "guardduty:GetDetector",
        "macie2:GetMacieSession",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "securityhub:DescribeHub",
        "securityhub:ListFindingAggregators",
        "inspector2:BatchGetAccountStatus",
        "detective:ListGraphs",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSecretsManagerClientReadOnlyAccess

Descrição: Fornece acesso para recuperar e descrever segredos do Secrets Manager. Essa política também permite descriptografar chaves KMS para segredos do Secrets Manager.

`AWSSecretsManagerClientReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSecretsManagerClientReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 05 de novembro de 2025, 20:04 UTC
- Horário editado: 02 de junho de 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecretsManagerClientReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerGetAndDescribeSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*"
    },
    {
      "Sid" : "SecretsManagerBatchGetSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:BatchGetSecretValue",
```

```
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSDecryptKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:*:secret:*",
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSecurityAgentServiceRolePolicy

Descrição: Permite que o AWS Security Agent gerencie recursos em seu nome.

`AWSSecurityAgentServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 11 de junho de 2026, 23:42 UTC
- Horário editado: 11 de junho de 2026, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityAgentServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LatticeCreateResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:CreateResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSSecurityAgentManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LatticeTagResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:TagResource"
      ],
```

```
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSSecurityAgentManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LatticeManageTaggedResourceGateways",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeleteResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSSecurityAgentManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LatticeGetResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:GetResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSSecurityAgentManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeApis",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CreateLatticeServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSecurityAgentWebAppPolicy

Descrição: Fornece permissões para usuários autenticados acessarem o aplicativo Web do Security Agent para configurar e executar testes automatizados de penetração de segurança. Essa política permite que os usuários gerenciem pentests, visualizem descobertas, monitorem a execução de testes e interajam com AWS os recursos necessários para operações de teste de segurança.

`AWSSecurityAgentWebAppPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSecurityAgentWebAppPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 05 de fevereiro de 2026, 23:19 UTC
- Horário editado: 24 de setembro de 2026, 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSecurityAgentWebAppPolicy`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:ListAgentSpaces",
        "securityagent:ListSecurityRequirements",
        "securityagent:ListTargetDomains",
        "securityagent:BatchGetTargetDomains"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentSpaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:AddArtifact",
        "securityagent:CreateThreat",
        "securityagent:BatchDeleteCodeReviews",
        "securityagent:BatchDeletePentests",
        "securityagent:BatchDeleteThreatModels",
        "securityagent:BatchGetAgentSpaces",
        "securityagent:BatchGetArtifactMetadata",
        "securityagent:BatchGetCodeReviewJobs",
        "securityagent:BatchGetCodeReviewJobTasks",
        "securityagent:BatchGetCodeReviews",
```

```
        "securityagent:BatchGetFindings",
        "securityagent:BatchGetPentestJobContentMetadata",
        "securityagent:BatchGetPentestJobs",
        "securityagent:BatchGetPentestJobTasks",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetThreatModelJobs",
        "securityagent:BatchGetThreatModelJobTasks",
        "securityagent:BatchGetThreatModels",
        "securityagent:BatchGetThreats",
        "securityagent:BatchGetValidationRuns",
        "securityagent:CreateCodeReview",
        "securityagent:CreateDesignReview",
        "securityagent:CreatePentest",
        "securityagent:CreateThreatModel",
        "securityagent:DeleteArtifact",
        "securityagent:DeleteDesignReview",
        "securityagent:GetArtifact",
        "securityagent:GetDesignReview",
        "securityagent:GetDesignReviewArtifact",
        "securityagent:GetDesignReviewFeedback",
        "securityagent:ListActorMessages",
        "securityagent:ListArtifacts",
        "securityagent:ListCodeReviewJobsForCodeReview",
        "securityagent:ListCodeReviewJobTasks",
        "securityagent:ListCodeReviews",
        "securityagent:ListDesignReviewComments",
        "securityagent:ListDesignReviews",
        "securityagent:ListDiscoveredDomains",
        "securityagent:ListDiscoveredEndpoints",
        "securityagent:ListFindings",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentestJobsForPentest",
        "securityagent:ListPentestJobTasks",
        "securityagent:ListPentests",
        "securityagent:ListThreatModelJobs",
        "securityagent:ListThreatModelJobTasks",
        "securityagent:ListThreatModels",
        "securityagent:ListThreats",
        "securityagent:PutDesignReviewFeedback",
        "securityagent:StartCodeRemediation",
        "securityagent:StartCodeReviewJob",
        "securityagent:StartPentestJob",
        "securityagent:StartThreatModelJob",
        "securityagent:StartValidationRun",
```

```
        "securityagent:StopCodeReviewJob",
        "securityagent:StopPentestJob",
        "securityagent:StopThreatModelJob",
        "securityagent:UpdateCodeReview",
        "securityagent:UpdateDiscoveredDomains",
        "securityagent:UpdateFinding",
        "securityagent:UpdatePentest",
        "securityagent:UpdateThreat",
        "securityagent:UpdateThreatModel"
      ],
      "Resource" : "arn:aws:securityagent:*:*:agent-space*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSecurityHubFullAccess

Descrição: Fornece acesso total para usar o AWS Security Hub.

`AWSSecurityHubFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSecurityHubFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 27 de novembro de 2018, 23:54 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubFullAccess`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubAllowAll",
      "Effect" : "Allow",
      "Action" : "securityhub:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "securityhub.amazonaws.com",
            "securityhubv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OtherServicePermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "guardduty:UpdateDetector",
        "guardduty:EnableOrganizationAdminAccount",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:DeleteDetector",
        "guardduty:CreateDetector",
        "guardduty:CreateMembers",
        "guardduty:UpdateOrganizationConfiguration",
        "guardduty:DescribeOrganizationConfiguration",
        "inspector2:BatchGetAccountStatus",
        "inspector2:Enable",
        "inspector2:Disable",
        "inspector2:EnableDelegatedAdminAccount",
        "inspector2:DisableDelegatedAdminAccount",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:UpdateOrganizationConfiguration",
        "inspector2:DescribeOrganizationConfiguration",
        "pricing:GetProducts",
        "account:ListRegions",
        "account:GetRegionOptStatus",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSecurityHubOrganizationsAccess

Descrição: Concede permissão para ativar e gerenciar o AWS Security Hub em uma organização. Inclui habilitar o serviço em toda a organização e determinar a conta de administrador delegado para o serviço.

`AWSSecurityHubOrganizationsAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSecurityHubOrganizationsAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de março de 2021, 20:53 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
```

```
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:DescribeResourcePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationPermissionsEnable",
      "Effect" : "Allow",
      "Action" : "organizations:EnableAWSServiceAccess",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com",
            "inspector2.amazonaws.com",
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationPermissionsDelegatedAdmin",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:account/o-*/*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com",
            "inspector2.amazonaws.com",
            "guardduty.amazonaws.com",
```

```
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationPolicyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource" : [
        "arn:aws:organizations::*:root/o-*/*",
        "arn:aws:organizations::*:account/o-*/*",
        "arn:aws:organizations::*:ou/o-*/*",
        "arn:aws:organizations::*:policy/o-*/securityhub_policy/*",
        "arn:aws:organizations::*:policy/o-*/inspector_policy/*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:PolicyType" : [
            "SECURITYHUB_POLICY",
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationPolicyTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:TagResource",
        "organizations:UntagResource",
        "organizations:ListTagsForResource"
      ],
      "Resource" : [
```

```
        "arn:aws:organizations::*:policy/o-*/securityhub_policy/*",
        "arn:aws:organizations::*:policy/o-*/inspector_policy/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSecurityHubReadOnlyAccess

Descrição: Fornece acesso somente para leitura aos recursos do AWS Security Hub

`AWSSecurityHubReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSecurityHubReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de novembro de 2018, 1:34 UTC
- Hora da edição: 22 de fevereiro de 2024, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSecurityHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:Get*",
        "securityhub:List*",
        "securityhub:BatchGet*",
        "securityhub:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSecurityHubServiceRolePolicy

Descrição: É necessária uma função vinculada ao serviço para que o AWS Security Hub acesse seus recursos.

`AWSSecurityHubServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 27 de novembro de 2018, 23:47 UTC
- Horário editado: 27 de junho de 2026, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy`

Versão da política

Versão da política: v16 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "logs:DescribeMetricFilters",
        "sns:ListSubscriptionsByTopic",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:BatchGetResourceConfig",
        "config:SelectResourceConfig",
        "iam:GenerateCredentialReport",
        "organizations:ListAccounts",
```

```
        "config:PutEvaluations",
        "tag:GetResources",
        "iam:GetCredentialReport",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "securityhub:BatchDisableStandards",
        "securityhub:BatchEnableStandards",
        "securityhub:BatchUpdateStandardsControlAssociations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:CreateMembers",
        "securityhub:DeleteMembers",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandards",
        "securityhub:DescribeStandardsControls",
        "securityhub:DisassociateFromAdministratorAccount",
        "securityhub:DisassociateMembers",
        "securityhub:DisableSecurityHub",
        "securityhub:EnableSecurityHub",
        "securityhub:GetEnabledStandards",
        "securityhub:ListStandardsControlAssociations",
        "securityhub:ListSecurityControlDefinitions",
        "securityhub:UpdateOrganizationConfiguration",
        "securityhub:UpdateSecurityControl",
        "securityhub:UpdateSecurityHubConfiguration",
        "securityhub:UpdateStandardsControl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceRoleConfigPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
    },
    {
```

```
      "Sid" : "SecurityHubServiceRoleOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecurityHubCSPMServiceRoleConfig",
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:PutThirdPartyServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
*ConfigurationRecorderForSecurityHubCSPM*"
      ]
    },
    {
      "Sid" : "SecurityHubCSPMServiceRoleConfigListAndGet",
      "Effect" : "Allow",
      "Action" : [
        "config:ListConfigurationRecorders",
        "config:GetConnector"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubCSPMServiceRoleIamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityHubCSPMServiceRoleConfigMetricsPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSecurityHubV2ServiceRolePolicy

Descrição: Essa política permite que o Security Hub gerencie as regras de AWS configuração e os recursos do Security Hub em sua organização e em seu nome.

`AWSSecurityHubV2ServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 10 de junho de 2025, 17:37 UTC
- Horário editado: 27 de junho de 2026, 00:42 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubV2ServiceRolePolicy`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubV2ServiceRoleAssetsConfig",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutServiceLinkedConfigurationRecorder",
        "config:PutThirdPartyServiceLinkedConfigurationRecorder"
      ],
      "Resource" : "arn:aws:config:*:*:configuration-recorder/
*ConfigurationRecorderForSecurityHubAssets*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleAssetsConfigListAndGet",
      "Effect" : "Allow",
      "Action" : [
        "config:ListConfigurationRecorders",
        "config:GetConnector"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleAssetsIamPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleSecurityHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:DisableSecurityHubV2",
        "securityhub:EnableSecurityHubV2",
        "securityhub:DescribeSecurityHubV2",
        "securityhub:EnableSecurityHubFeatureV2",
        "securityhub:DisableSecurityHubFeatureV2"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hubv2/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleOrganizationsPermissionsOnResources",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "arn:aws:organizations::*:*"
    },
```

```
    {
      "Sid" : "SecurityHubV2ServiceRoleOrganizationsPermissionsWithoutResources",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleDelegatedAdminPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleEcrListingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeImages",
        "ecr:DescribeRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleLambdaAndConfigMetricPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SecurityHubV2ServiceRoleLambdaListingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleIamListingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetAccountSummary"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleIA2IamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/access-analyzer.amazonaws.com/
AWSServiceRoleForAccessAnalyzer"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "access-analyzer.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleIA2ResAPermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CreateServiceLinkedAnalyzer",
        "access-analyzer:DeleteServiceLinkedAnalyzer"
      ],
      "Resource" : "arn:*:access-analyzer:*:*:analyzer/*"
    },
    {
```

```
      "Sid" : "SecurityHubV2ServiceRoleIA2ResAListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleIA2APIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetFindingRecommendation",
        "access-analyzer:GenerateFindingRecommendation"
      ],
      "Resource" : "arn:*:access-analyzer:*:*:analyzer/
_AccessAnalyzerForSecurityHubV2*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleAPIPolicyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GetUserPolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*",
        "arn:aws:iam::*:user/*"
      ]
    },
    {
      "Sid" : "SecurityHubConnectorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:CreateConnector",
        "securityhub:UpdateConnector",
        "securityhub:DeleteConnector"
      ],
      "Resource" : "arn:aws:securityhub:*:*:connector/*",
      "Condition" : {
        "StringLikeIfExists" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleInspectorConnectorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:CreateConnector",
        "inspector2:DeleteConnector",
        "inspector2:ListConnectors",
        "inspector2:ListConnectorScanConfigurations",
        "inspector2:UpdateConnector",
        "inspector2:UpdateConnectorScanConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleInspectorIamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
thirdparty.inspector2.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "thirdparty.inspector2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleOutboundIdentityFederationPermission",
      "Effect" : "Allow",
      "Action" : "sts:GetWebIdentityToken",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "sts:IdentityTokenAudience" : [
            "api://AzureADTokenExchange"
```

```
            ]
          }
        }
      }
    ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSecurityIncidentResponseCaseFullAccess

Descrição: a política fornece aos clientes permissões de leitura e gravação para os recursos dos casos criados por meio do serviço do Security Incident Response.

`AWSSecurityIncidentResponseCaseFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSecurityIncidentResponseCaseFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Tempo de criação: 01 de dezembro de 2024, 23:21 UTC
- Horário editado: 22 de abril de 2026, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseCaseFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRCaseFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetCase",
        "security-ir:ListCases",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:ListComments",
        "security-ir:ListCaseEdits",
        "security-ir:CreateCase",
        "security-ir:UpdateCase",
        "security-ir:CloseCase",
        "security-ir:UpdateCaseStatus",
        "security-ir:UpdateResolverType",
        "security-ir:GetCaseAttachmentUploadUrl",
        "security-ir:CreateCaseComment",
        "security-ir:UpdateCaseComment",
        "security-ir:SendFeedback",
        "security-ir:ListInvestigations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityIRCaseTagFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:ListTagsForResource",
        "security-ir:TagResource",
        "security-ir:UntagResource"
      ],
      "Resource" : "arn:aws:security-ir:*:*:case/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSecurityIncidentResponseFullAccess

Descrição: a política concede aos clientes permissões de leitura e gravação para todos os recursos associados ao serviço do Security Incident Response.

`AWSSecurityIncidentResponseFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSecurityIncidentResponseFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Tempo de criação: 01 de dezembro de 2024, 23:21 UTC
- Horário editado: 22 de abril de 2026, 16:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForSecurityIncidentResponse",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/security-ir.amazonaws.com/
AWSServiceRoleForSecurityIncidentResponse"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "security-ir.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForSecurityIncidentResponseTriage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/triage.security-ir.amazonaws.com/
AWSServiceRoleForSecurityIncidentResponse_Triage"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "triage.security-ir.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OrganizationsPolicies",
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSecurityIncidentResponseReadOnlyAccess

Descrição: A política fornece aos clientes Read-only permissões para todos os recursos associados ao serviço de Resposta a Incidentes de Segurança. A permissão também inclui acesso GetCaseAttachmentDownloadUrl à capacidade de obter URLs de download de anexos de casos.

`AWSSecurityIncidentResponseReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSecurityIncidentResponseReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Tempo de criação: 01 de dezembro de 2024, 23:06 UTC
- Horário editado: 01 de outubro de 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseReadOnlyAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:BatchGetMemberAccountDetails",
        "security-ir:GetMembership",
        "security-ir:ListMemberships",
        "security-ir:GetCase",
        "security-ir:ListCases",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:ListComments",
        "security-ir:ListCaseEdits",
        "security-ir:ListTagsForResource",
        "security-ir:ListInvestigations",
        "security-ir:GetFindingMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSecurityIncidentResponseServiceRolePolicy

Descrição: Fornece acesso aos AWS recursos gerenciados ou usados pelo Security Incident Response

`AWSSecurityIncidentResponseServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 01 de dezembro de 2024, 16:36 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseServiceRolePolicy`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIncidentResponseOrganizationsPolicy",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityIncidentResponseCreateCasePolicyTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:TagResource",
        "security-ir:CreateCase"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SecurityIncidentResponseManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SecurityIncidentResponseManaged" : "true",
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      },
      "Resource" : "arn:aws:security-ir:*:*:case/*"
    },
    {
      "Sid" : "SecurityIncidentResponseOperationsPolicy",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetCase",
        "security-ir:UpdateCase",
        "security-ir:ListCases",
```

```
        "security-ir:CreateCaseComment",
        "security-ir:ListComments"
      ],
      "Resource" : "arn:aws:security-ir:*:*:case/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSecurityIncidentResponseTriageServiceRolePolicy

Descrição: Fornece acesso ao AWS Security Incident Response para monitorar continuamente seu ambiente em busca de ameaças à segurança, ajustar os serviços de segurança para reduzir o ruído de alerta e coletar informações para investigar possíveis incidentes.

`AWSSecurityIncidentResponseTriageServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 01 de dezembro de 2024, 16:36 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseTriageServiceRolePolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "triage.security-ir.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "guardduty:ArchiveFindings",
        "guardduty:CreateFilter",
        "guardduty:DescribeMalwareScans",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:StartMalwareScan",
        "guardduty:UpdateFindingsFeedback"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "securityhub:BatchUpdateFindings",
        "securityhub:DescribeHub",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindings",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:UpdateFindings"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hub/default"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:CreateCase",
        "security-ir:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SecurityIncidentResponseManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SecurityIncidentResponseManaged" : "true",
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:UpdateCase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetMembership",
        "security-ir:ListMemberships"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceCatalogAdminFullAccess

Descrição: fornece acesso total aos recursos administrativos do Service Catalog

`AWSServiceCatalogAdminFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSServiceCatalogAdminFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de fevereiro de 2018, 17:19 UTC
- Horário editado: 04 de agosto de 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:CreateStackSet",
        "cloudformation:CreateStackInstances",
        "cloudformation:UpdateStackSet",
```

```
        "cloudformation:UpdateStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateUploadBucket",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ValidateTemplate",
        "iam:GetGroup",
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "servicecatalog:Get*",
        "servicecatalog:Scan*",
        "servicecatalog:Search*",
        "servicecatalog:List*",
        "servicecatalog:TagResource",
        "servicecatalog:UntagResource",
        "servicecatalog:SyncResource",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:Accept*",
        "servicecatalog:Associate*",
        "servicecatalog:Batch*",
        "servicecatalog:Copy*",
        "servicecatalog:Create*",
        "servicecatalog:Delete*",
        "servicecatalog:Describe*",
        "servicecatalog:Disable*",
        "servicecatalog:Disassociate*",
        "servicecatalog:Enable*",
        "servicecatalog:Execute*",
        "servicecatalog:Import*",
        "servicecatalog:Provision*",
        "servicecatalog:Put*",
        "servicecatalog:Reject*",
        "servicecatalog:Terminate*",
        "servicecatalog:Update*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "servicecatalog.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
orgsdatasync.servicecatalog.amazonaws.com/AWSServiceRoleForServiceCatalogOrgsDataSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "orgsdatasync.servicecatalog.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceCatalogAdminReadOnlyAccess

Descrição: fornece acesso somente leitura aos recursos administrativos do Service Catalog

`AWSServiceCatalogAdminReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSServiceCatalogAdminReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de outubro de 2019, 18:53 UTC
- Hora da edição: 25 de outubro de 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "iam:GetGroup",
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "servicecatalog:Get*",
        "servicecatalog:List*",
        "servicecatalog:Describe*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:Search*",
        "ssm:DescribeDocument",
```

```
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceCatalogAppRegistryFullAccess

Descrição: fornece acesso total aos recursos do Service Catalog AppRegistry

`AWSServiceCatalogAppRegistryFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSServiceCatalogAppRegistryFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 12 de novembro de 2020, 22:25 UTC
- Horário editado: 12 de agosto de 2026, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppRegistryUpdateStackAndResourceGroupTagging",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
        },
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "UpdateStack"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AppRegistryResourceGroupsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "resource-groups:GetGroup",
        "resource-groups:GetTags",
        "resource-groups:Tag",
        "resource-groups:Untag",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:AssociateResource",
        "resource-groups:DisassociateResource"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/AWS_*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRegistryServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRegistryOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "servicecatalog:CreateApplication",
        "servicecatalog:GetApplication",
        "servicecatalog:UpdateApplication",
```

```
        "servicecatalog:DeleteApplication",
        "servicecatalog:ListApplications",
        "servicecatalog:AssociateResource",
        "servicecatalog:DisassociateResource",
        "servicecatalog:GetAssociatedResource",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup",
        "servicecatalog:ListAssociatedAttributeGroups",
        "servicecatalog:CreateAttributeGroup",
        "servicecatalog:UpdateAttributeGroup",
        "servicecatalog:DeleteAttributeGroup",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:SyncResource",
        "servicecatalog:ListAttributeGroupsForApplication",
        "servicecatalog:GetConfiguration",
        "servicecatalog:PutConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AppRegistryResourceTagging",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListTagsForResource",
        "servicecatalog:UntagResource",
        "servicecatalog:TagResource"
      ],
      "Resource" : "arn:aws:servicecatalog:*:*:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceCatalogAppRegistryReadOnlyAccess

Descrição: fornece acesso somente leitura aos recursos Service Catalog AppRegistry

`AWSServiceCatalogAppRegistryReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSServiceCatalogAppRegistryReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 12 de novembro de 2020, 22:34 UTC
- Hora da edição: 17 de novembro de 2022, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:GetApplication",
        "servicecatalog:ListApplications",
        "servicecatalog:GetAssociatedResource",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAssociatedAttributeGroups",
```

```
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListTagsForResource",
        "servicecatalog:ListAttributeGroupsForApplication",
        "servicecatalog:GetConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceCatalogAppRegistryServiceRolePolicy

Descrição: permite que o Service Catalog AppRegistry gerencie grupos de recursos em seu nome

`AWSServiceCatalogAppRegistryServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 18 de maio de 2021, 22:18 UTC
- Hora da edição: 26 de outubro de 2022, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:DescribeStacks",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:DeleteGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:GetTags",
        "resource-groups:Tag",
        "resource-groups:Untag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration"
      ],
      "Resource" : [
        "arn:*:resource-groups:*:*:group/AWS_AppRegistry*",
        "arn:*:resource-groups:*:*:group/AWS_CloudFormation_Stack*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceCatalogEndUserFullAccess

Descrição: fornece acesso total aos recursos de usuário final do Service Catalog

`AWSServiceCatalogEndUserFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSServiceCatalogEndUserFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de fevereiro de 2018, 17:22 UTC
- Horário editado: 04 de agosto de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:ValidateTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DeleteChangeSet",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:CreateStackSet",
        "cloudformation:CreateStackInstances",
        "cloudformation:UpdateStackSet",
        "cloudformation:UpdateStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
```

```
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:ProvisionProduct",
        "servicecatalog:SearchProducts",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DescribeProvisionedProduct",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:ListStackInstancesForProvisionedProduct",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:CreateProvisionedProductPlan",
        "servicecatalog:DescribeProvisionedProductPlan",
        "servicecatalog:ExecuteProvisionedProductPlan",
        "servicecatalog:DeleteProvisionedProductPlan",
        "servicecatalog:ListProvisionedProductPlans",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:ExecuteProvisionedProductServiceAction",
        "servicecatalog:DescribeServiceActionExecutionParameters"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceCatalogEndUserReadOnlyAccess

Descrição: fornece acesso somente leitura aos recursos de usuário final do Service Catalog

`AWSServiceCatalogEndUserReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSServiceCatalogEndUserReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de outubro de 2019, 18:49 UTC
- Hora da edição: 25 de outubro de 2019, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListLaunchPaths",
```

```
        "servicecatalog:SearchProducts",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DescribeProvisionedProduct",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:ListStackInstancesForProvisionedProduct",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:DescribeProvisionedProductPlan",
        "servicecatalog:ListProvisionedProductPlans",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeServiceActionExecutionParameters"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

Descrição: Uma política de função vinculada a serviços para AWS ServiceCatalog sincronizar com a estrutura AWS organizacional da organização

`AWSServiceCatalogOrgsDataSyncServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 10 de abril de 2023, 20:48 UTC
- Horário editado: 08 de dezembro de 2025, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
```

```
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalogRegions",
      "Effect" : "Allow",
      "Action" : [
        "account:ListRegions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceCatalogSyncServiceRolePolicy

Descrição: Uma função vinculada ao serviço para AWS ServiceCatalog sincronizar artefatos de provisionamento dos repositórios de origem

`AWSServiceCatalogSyncServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 15 de novembro de 2022, 21:20 UTC
- Hora da edição: 03 de maio de 2024, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListProvisioningArtifacts",
        "servicecatalog:DescribeProductAsAdmin",
        "servicecatalog:DeleteProvisioningArtifact",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeProvisioningArtifact",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:UpdateProvisioningArtifact"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessArtifactRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
```

```
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "ValidateTemplate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForAIDevOpsPolicy

Descrição: Essa função vinculada ao serviço fornece a AIDevOps capacidade de fornecer informações de uso.

`AWSServiceRoleForAIDevOpsPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 16 de fevereiro de 2026, 14:27 UTC

- Horário editado: 27 de março de 2026, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAIDevOpsPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/AIDevOps"
          ]
        }
      }
    },
    {
      "Sid" : "LatticeCreateResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:CreateResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/AWSAIDevOpsManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LatticeTagResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:TagResource"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSAIDevOpsManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LatticeManageTaggedResourceGateways",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeleteResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSAIDevOpsManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LatticeGetResourceGateway",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:GetResourceGateway"
      ],
      "Resource" : "arn:aws:vpc-lattice:*:*:resourcegateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSAIDevOpsManaged" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "DescribeApis",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateLatticeServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForAmazonEKSNodegroup

Descrição: permissões necessárias para gerenciar grupos de nós na conta do cliente. Essas políticas estão relacionadas ao gerenciamento dos seguintes recursos: AutoscalingGroups SecurityGroups, LaunchTemplates InstanceProfiles e.

`AWSServiceRoleForAmazonEKSNodegroup` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 07 de novembro de 2019, 1:34 UTC
- Horário editado: 17 de fevereiro de 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SharedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "ec2:ResourceTag/eks" : "*"
        }
      }
    },
    {
      "Sid" : "EKSCreatedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "LaunchTemplateRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "AutoscalingRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
```

```
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:PutLifecycleHook",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:EnableMetricsCollection",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:PutWarmPool",
        "autoscaling:DeleteWarmPool"
      ],
      "Resource" : "arn:aws:autoscaling:*:*:*:autoScalingGroupName/eks-*"
    },
    {
      "Sid" : "AllowAutoscalingToCreateSLR",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      },
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowASGCreationByEKS",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:CreateAutoScalingGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToAutoscaling",
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToManageResourcesForNodegroups",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "ec2:CreateLaunchTemplate",
        "ec2:DescribeInstances",
        "iam:GetInstanceProfile",
        "ec2:DescribeLaunchTemplates",
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:RunInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:GetConsoleOutput",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeCapacityReservations",
        "autoscaling:DescribeWarmPool"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "PermissionsToCreateAndManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-*"
    },
    {
      "Sid" : "PermissionsToDeleteEKSAndKubernetesTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsForManagedNodegroupsAutoRepair",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "PermissionsToCreateEKSAndKubernetesTags",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:security-group/*",
        "arn:*:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowTaggingEC2ResourcesOnlyDuringInstanceCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:instance/*",
        "arn:*:ec2:*:*:volume/*",
        "arn:*:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
```

```
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForAmazonQDeveloper

Descrição: este perfil vinculado ao serviço fornece ao Amazon Q Developer a capacidade de fornecer informações de utilização.

`AWSServiceRoleForAmazonQDeveloper` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 25 de abril de 2024, 7:40 UTC
- Horário editado: 20 de julho de 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonQDeveloper`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Q"
          ]
        }
      }
    },
    {
      "Sid" : "sid2",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForAWSTransform

Descrição: Essa Service-Linked função fornece ao AWS Transform a capacidade de fornecer informações de uso.

`AWSServiceRoleForAWSTransform` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 15 de maio de 2025, 13:37 UTC
- Horário editado: 12 de fevereiro de 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAWSTransform`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PublishCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Transform"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "UserManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication",
        "sso:GetApplicationAssignmentConfiguration",
        "sso:ListApplicationAssignmentsForPrincipal"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SupportCaseManagement",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:AddCommunicationToCase",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExternalIdpSecretsAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:transform!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "transform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForAWSTransformCustom

Descrição: permite que o AWS Transform Custom publique CloudWatch métricas em sua conta em seu nome.

`AWSServiceRoleForAWSTransformCustom` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Tempo de criação: 25 de março de 2026, 02:57 UTC
- Horário editado: 05 de maio de 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAWSTransformCustom`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/TransformCustom"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/TransformCustom",
        "arn:aws:logs:*:*:log-group:/aws/TransformCustom:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

Descrição: Fornece acesso aos recursos do Systems Manager usados pelos CloudWatch alarmes

`AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 1º de outubro de 2020, 9:49 UTC
- Hora da edição: 1º de outubro de 2020, 9:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePoli

Descrição: Permite CloudWatch acessar as métricas do RDS Performance Insights em seu nome

`AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 7 de setembro de 2023, 9:32 UTC
- Hora da edição: 7 de setembro de 2023, 9:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForCodeGuru-Profiler

Descrição: É necessária uma função vinculada ao serviço para que o Amazon CodeGuru Profiler envie notificações em seu nome.

`AWSServiceRoleForCodeGuru-Profiler` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 26 de junho de 2020, 22:04 UTC
- Hora da edição: 26 de junho de 2020, 22:04 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSNSPublishToSendNotifications",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForCodeWhispererPolicy

Descrição: Essa função concede permissões CodeWhisperer para acessar dados em sua conta para calcular o faturamento, fornece acesso para criar e acessar relatórios de segurança na Amazon CodeGuru e emitir dados para. CloudWatch

`AWSServiceRoleForCodeWhispererPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 24 de março de 2023, 19:39 UTC
- Horário editado: 09 de abril de 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid2",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListDirectoryAssociations",
        "sso:DescribeRegisteredRegions",
        "sso:GetProfile",
        "sso:GetManagedApplicationInstance",
        "sso:ListApplicationAssignments",
        "sso:DescribeInstance",
        "sso:DescribeApplication"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid3",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateUploadUrl"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid4",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:GetScan",
        "codeguru-security:ListFindings",
        "codeguru-security:GetFindings"
      ],
      "Resource" : [
        "arn:aws:codeguru-security:*:*:scans/CodeWhisperer-*"
      ]
    },
    {
      "Sid" : "sid5",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/CodeWhisperer"
          ]
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForEC2ScheduledInstances

Descrição: permite que instâncias programadas do EC2 iniciem e gerenciem instâncias spot.

`AWSServiceRoleForEC2ScheduledInstances` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 12 de outubro de 2017, 18:31 UTC
- Hora da edição: 12 de outubro de 2017, 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:ec2sri:scheduledInstanceId"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2sri:scheduledInstanceId" : "*"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Descrição: AWS GroundStation usa essa função vinculada ao serviço para invocar o EC2 para encontrar endereços IPv4 públicos

`AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 13 de dezembro de 2022, 23:52 UTC
- Hora da edição: 13 de dezembro de 2022, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForImageBuilder

Descrição: Permite ligar EC2ImageBuilder para AWS os serviços em seu nome.

`AWSServiceRoleForImageBuilder` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 29 de novembro de 2019, 22:02 UTC
- Horário editado: 09 de julho de 2026, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder`

Versão da política

Versão da política: v28 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:RegisterImage",
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RegisterImage",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "vmie.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateLaunchTemplate",
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeSnapshots",
        "ec2:DescribeHosts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateImage"
          ],
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:export-image-task/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:AddTagsToResource",
        "ssm:DescribeInstanceInformation",
        "ssm:GetAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListInventoryEntries",
        "ssm:SendAutomationSignal",
        "ssm:DescribeInstanceAssociationsStatus",
        "ssm:DescribeAssociationExecutions",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ssm:*:*:document/AWSEC2-RunSysprep",
        "arn:aws:s3:::*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/CreatedBy" : [
            "EC2 Image Builder"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        },
        "StringLike" : {
```

```
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/EC2ImageBuilderDistributionCrossAccountRole"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
```

```
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplates",
        "ec2:ModifyLaunchTemplate",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : "arn:aws:ec2:*:*:export-image-task/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelExportTask"
      ],
      "Resource" : "arn:aws:ec2:*:*:export-image-task/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ssm.amazonaws.com",
            "ec2fastlaunch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachImageWatermark"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "inspector2:ListCoverage",
        "inspector2:ListFindings"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:TagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchDeleteImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
      "Condition" : {
        "StringEquals" : {
          "ecr:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/ImageBuilder-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/imagebuilder/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "imagebuilder:StartImagePipelineExecution",
      "Resource" : "arn:aws:imagebuilder:*:*:image-pipeline/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "imagebuilder:TagResource",
      "Resource" : "arn:aws:imagebuilder:*:*:image-pipeline/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForIoTSiteWise

Descrição: permite que SiteWise a AWS IoT provisione e gerencie gateways, bem como dados de consulta. A política inclui as permissões necessárias do AWS Greengrass para implantação em grupos, permissões do AWS Lambda para criar e atualizar funções prefixadas pelo serviço e permissões do AWS IoT Analytics para consultar dados de armazenamentos de dados.

`AWSServiceRoleForIoTSiteWise` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 14 de novembro de 2018, 19:19 UTC
- Hora da edição: 13 de novembro de 2023, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSiteWiseReadGreenGrass",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:GetAssociatedRole",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLog",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*:log-stream:*"
    },
    {
      "Sid" : "AllowSiteWiseAccessSiteWiseManagedWorkspaceInTwinMaker",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ExecuteQuery"
      ],
      "Resource" : "arn:aws:iottwinmaker:*:*:workspace/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITEWISE"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForLogDeliveryPolicy

Descrição: permite que o serviço de entrega de logs entregue logs chamando o destino do log em seu nome.

`AWSServiceRoleForLogDeliveryPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 04 de outubro de 2019, 17:31 UTC
- Horário editado: 15 de maio de 2026, 21:57 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LogDeliveryToFirehose",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
        }
      }
    },
    {
      "Sid" : "KMSForFirehoseSSECMK",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "firehose.*.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForMonitronPolicy

Descrição: Concede ao Amazon Monitron permissões para gerenciar AWS recursos, incluindo a atribuição de usuários de AWS SSO em seu nome.

`AWSServiceRoleForMonitronPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 02 de dezembro de 2020, 19:06 UTC
- Horário editado: 07 de janeiro de 2026, 09:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:GetProfile",
        "sso:ListProfiles",
        "sso:ListProfileAssociations",
        "sso:AssociateProfile",
        "sso:ListDirectoryAssociations",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "sso:CreateApplicationAssignment",
        "sso:ListApplicationAssignments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForNeptuneGraphPolicy

Descrição: fornece acesso ao Cloudwatch para publicar métricas e logs operacionais e de uso para o Amazon Neptune

`AWSServiceRoleForNeptuneGraphPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 29 de novembro de 2023, 14:03 UTC

- Hora da edição: 29 de novembro de 2023, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GraphMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Neptune",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Sid" : "GraphLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GraphLogEvents",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForPrivateMarketplaceAdminPolicy

Descrição: fornece permissões para descrever e atualizar os recursos do Private Marketplace e descrever AWS organizações

`AWSServiceRoleForPrivateMarketplaceAdminPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 14 de fevereiro de 2024, 22:28 UTC
- Hora da edição: 14 de fevereiro de 2024, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceCatalogDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Audience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProcurementPolicy/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/BrandingSettings/*"
      ]
    },
```

```
    {
      "Sid" : "PrivateMarketplaceCatalogDescribeChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceCatalogListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceStartChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
            "AssociateAudience",
            "DisassociateAudience"
          ]
        }
      },
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceOrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListChildren"
```

```
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForProcurementInsightsPolicy

Descrição: política de insights de compras para obter detalhes da conta da organização

`AWSServiceRoleForProcurementInsightsPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 3 de outubro de 2024, 14:26 UTC
- Hora da edição: 3 de outubro de 2024, 14:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForProcurementInsightsPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProcurementInsightsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForSMS

Descrição: Fornece acesso aos AWS serviços e recursos necessários para migrar instâncias de serviço, AWS incluindo EC2, S3 e Cloudformation.

`AWSServiceRoleForSMS` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 06 de agosto de 2019, 18:39 UTC
- Hora da edição: 15 de outubro de 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*",
      "Condition" : {
        "Null" : {
          "cloudformation:ResourceTypes" : "false"
        },
        "ForAllValues:StringEquals" : {
          "cloudformation:ResourceTypes" : [
            "AWS::EC2::Instance",
```

```
            "AWS::ApplicationInsights::Application",
            "AWS::ResourceGroups::Group"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::sms-app-*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:CreateReplicationJob",
        "sms:DeleteReplicationJob",
        "sms:GetReplicationJobs",
        "sms:GetReplicationRuns",
        "sms:GetServers",
        "sms:ImportServerCatalog",
        "sms:StartOnDemandReplicationRun",
        "sms:UpdateReplicationJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:s3:::sms-app-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/UseForSMSApplicationValidation" : [
            "true"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotAttribute",
```

```
        "ec2:DeregisterImage",
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "cloudformation.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
```

```
        "applicationinsights:List*",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:CreateApplication",
        "applicationinsights:CreateComponent",
        "applicationinsights:UpdateApplication",
        "applicationinsights:DeleteApplication",
        "applicationinsights:UpdateComponentConfiguration",
        "applicationinsights:DeleteComponent"
      ],
      "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRoleForUserSubscriptions

Descrição: fornece acesso para o serviço de assinaturas de usuários aos recursos do Centro de Identidade para atualizar automaticamente suas assinaturas.

`AWSServiceRoleForUserSubscriptions` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 25 de abril de 2024, 16:14 UTC
- Horário editado: 22 de junho de 2026, 08:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForUserSubscriptions`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SubscriptionManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "organizations:DescribeOrganization",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso-directory:DescribeUser",
        "sso:ListApplicationAssignments"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRolePolicyForBackupReports

Descrição: Fornece permissões de AWS backup para criar relatórios de conformidade em seu nome

`AWSServiceRolePolicyForBackupReports` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Hora da criação: 19 de agosto de 2021, 21:16 UTC
- Hora da edição: 10 de março de 2023, 0:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeFramework",
        "backup:ListBackupJobs",
        "backup:ListRestoreJobs",
        "backup:ListCopyJobs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:BatchGetResourceConfig",
        "config:SelectResourceConfig",
        "config:DescribeConfigurationAggregators",
        "config:SelectAggregateResourceConfig",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "s3:GetBucketLocation"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/
backup.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
        "config:PutConfigurationAggregator"
      ],
      "Resource" : "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
backup.amazonaws.com*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRolePolicyForBackupRestoreTesting

Descrição: esta política contém permissões para testar restaurações e limpar recursos criados durante os testes.

`AWSServiceRolePolicyForBackupRestoreTesting` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 10 de novembro de 2023, 23:37 UTC
- Horário editado: 25 de setembro de 2026, 01:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BackupActions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeRecoveryPoint",
        "backup:DescribeRestoreJob",
        "backup:DescribeProtectedResource",
        "backup:GetRecoveryPointRestoreMetadata",
        "backup:ListBackupVaults",
        "backup:ListProtectedResources",
        "backup:ListProtectedResourcesByBackupVault",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListRecoveryPointsByResource",
        "backup:ListTags",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "IamPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:TerminateInstances",
        "elasticfilesystem:DeleteFilesystem",
        "elasticfilesystem:DeleteMountTarget",
        "rds:DeleteDBCluster",
        "rds:DeleteDBInstance",
        "rds:DeleteTenantDatabase",
```

```
        "fsx:DeleteFileSystem",
        "fsx:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/awsbackup-restore-test" : "false"
        }
      }
    },
    {
      "Sid" : "DdbDeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/awsbackup-restore-test-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftDeleteActions",
      "Effect" : "Allow",
      "Action" : "redshift:DeleteCluster",
      "Resource" : "arn:aws:redshift:*:*:cluster:awsbackup-restore-test-*"
    },
    {
      "Sid" : "S3DeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::awsbackup-restore-test-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "TimestreamDeleteActions",
      "Effect" : "Allow",
      "Action" : "timestream:DeleteTable",
      "Resource" : "arn:aws:timestream:*:*:database/*/table/awsbackup-restore-test-*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSServiceRolePolicyForWorkspacesInstances

Descrição: Essa política gerenciada fornece acesso administrativo à Amazon WorkSpaces para gerenciar instâncias do EC2 em seu Conta da AWS

`AWSServiceRolePolicyForWorkspacesInstances` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 11 de junho de 2025, 20:37 UTC
- Horário editado: 27 de agosto de 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForWorkspacesInstances`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateCapacityReservation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateCapacityReservation",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ManagedBy" : "workspaces-instances"
        }
      }
    },
    {
      "Sid" : "ManageTaggedCapacityReservations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyCapacityReservation",
        "ec2:CancelCapacityReservation"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedBy" : "workspaces-instances"
        }
      }
    },
    {
      "Sid" : "TagRemediation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:capacity-reservation/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ManagedBy" : "workspaces-instances"
        }
      }
    },
    {
      "Sid" : "ManagedInstanceOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:TerminateInstances",
        "ec2:DeleteVolume",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ManagedResourceOperator" : "workspaces-instances.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSShieldDRTAccessPolicy

Descrição: Fornece à equipe de resposta a AWS DDoS acesso limitado a você Conta da AWS para ajudar na mitigação de ataques de DDoS durante um evento de alta gravidade.

`AWSShieldDRTAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSShieldDRTAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 05 de junho de 2018, 22:29 UTC
- Hora da edição: 15 de dezembro de 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SRTAccessProtectedResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:List*",
        "route53:List*",
        "elasticloadbalancing:Describe*",
        "cloudwatch:Describe*",
```

```
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudfront:GetDistribution*",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:DescribeAccelerator",
        "ec2:DescribeRegions",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SRTManageProtections",
      "Effect" : "Allow",
      "Action" : [
        "shield:*",
        "waf:*",
        "wafv2:*",
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "cloudfront:UpdateDistribution",
        "apigateway:SetWebACL"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSShieldServiceRolePolicy

Descrição: Permite que o AWS Shield acesse AWS recursos em seu nome para fornecer proteção contra DDoS.

`AWSShieldServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 17 de novembro de 2021, 19:17 UTC
- Hora da edição: 17 de novembro de 2021, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSocialMessagingServiceRolePolicy

Descrição: fornece acesso para publicar métricas e fornecer insights para o envio das suas mensagens sociais.

`AWSSocialMessagingServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 10 de outubro de 2024, 19:28 UTC
- Hora da edição: 10 de outubro de 2024, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSocialMessagingServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudwatchMetricPublishing",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/SocialMessaging"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSSMForSAPServiceLinkedRolePolicy

Descrição: Fornece ao AWS Systems Manager for SAP as permissões necessárias para gerenciar e integrar o software SAP com AWS o.

`AWSSSMForSAPServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Hora da criação: 16 de novembro de 2022, 1:18 UTC
- Horário editado: 12 de fevereiro de 2026, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

Versão da política

Versão da política: v21 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcs",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstanceStatus",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstanceStatus",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "TargetRuleActions",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:*:events:*:*:rule/SSMSAPManagedRule*",
        "arn:*:events:*:*:event-bus/default"
      ]
    },
    {
      "Sid" : "DocumentActions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:*:ssm:*:*:document/AWSSystemsManagerSAP-*",
        "arn:*:ssm:*:*:document/AWSSSMSAP*",
        "arn:*:ssm:*:*:document/AWSSAP*"
      ]
    },
    {
      "Sid" : "CustomerSendCommand",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ssm:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "InstanceTagActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
```

```
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/awsApplication" : "false"
        },
        "StringEqualsIgnoreCase" : {
          "ec2:ResourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "DescribeTag",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeTags",
      "Resource" : "*"
    },
    {
      "Sid" : "GetApplication",
      "Effect" : "Allow",
      "Action" : "servicecatalog:GetApplication",
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "UpdateOrDeleteApplication",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DeleteApplication",
        "servicecatalog:UpdateApplication"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateApplication",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TagResource",
        "servicecatalog:CreateApplication"
      ],
```

```
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Usage",
            "AWS/SSMForSAP"
          ]
        }
      }
    },
    {
      "Sid" : "CreateAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:CreateAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
```

```
    {
      "Sid" : "GetAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:GetAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*"
    },
    {
      "Sid" : "DeleteAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:DeleteAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "AttributeGroupActions",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "ListAssociatedAttributeGroups",
      "Effect" : "Allow",
      "Action" : "servicecatalog:ListAssociatedAttributeGroups",
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "CreateGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
```

```
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SSMForSAPCreated"
          ]
        }
      }
    },
    {
      "Sid" : "GetGroup",
      "Effect" : "Allow",
      "Action" : "resource-groups:GetGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*"
    },
    {
      "Sid" : "DeleteGroup",
      "Effect" : "Allow",
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "TagAppTagResourceGroup",
```

```
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:Tag"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "GetAppTagResourceGroupConfig",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupConfiguration"
      ],
      "Resource" : [
        "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*"
      ]
    },
    {
      "Sid" : "StartStopInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ec2:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "SsmSapResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:Tag",
        "resource-groups:CreateGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SSMForSAPCreated"
          ]
        }
      }
    },
    {
      "Sid" : "ManageSsmSapTagsOnEc2Instances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPManaged" : "True"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "SystemsManagerForSAP-*"
          ]
        }
      }
    },
    {
      "Sid" : "ManageSsmSapTagsOnEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "SystemsManagerForSAP-*"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "ManageAppTagsOnEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/awsApplication" : "arn:aws:resource-groups:*:*:group/*/*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "awsApplication"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCostAllocationTags",
      "Effect" : "Allow",
      "Action" : [
        "ce:ListCostAllocationTags",
        "ce:UpdateCostAllocationTagsStatus",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:StartCostAllocationTagBackfill"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSSMOpsInsightsServiceRolePolicy

Descrição: Política para função vinculada ao serviço AWSServiceRoleForAmazonSSM _ OpsInsights

`AWSSSMOpsInsightsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 16 de junho de 2021, 20:12 UTC
- Hora da edição: 16 de junho de 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateOpsItem",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:CreateOpsItem",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateOpsItem",
        "ssm:GetOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SsmOperationalInsight" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSSODirectoryAdministrator

Descrição: acesso de administrador ao SSO Directory

`AWSSSODirectoryAdministrator` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSSODirectoryAdministrator` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 31 de outubro de 2018, 23:54 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSSODirectoryReadOnly

Descrição: ReadOnly acesso ao Diretório SSO

`AWSSSODirectoryReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSSODirectoryReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 31 de outubro de 2018, 23:49 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:Search*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Get*",
        "identitystore:Describe*",
        "identitystore:List*",
        "identitystore-auth:ListSessions",
        "identitystore-auth:BatchGetSession"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSSOMasterAccountAdministrator

Descrição: Fornece acesso ao AWS SSO para gerenciar AWS as contas principais e de membros da organização e o aplicativo em nuvem

`AWSSSOMasterAccountAdministrator` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSSOMasterAccountAdministrator` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de junho de 2018, 20:36 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator`

Versão da política

Versão da política: v13 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
```

```
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMasterAccountAdministrator",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeTrusts",
        "ds:UnauthorizeApplication",
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy",
        "signin:CreateTrustedIdentityPropagationApplicationForConsole",
```

```
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowDeleteSyncProfile",
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile"
      ],
      "Resource" : [
        "arn:aws:identity-sync:*:*:profile/*"
      ]
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
      }
    },
```

```
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSSOMemberAccountAdministrator

Descrição: Fornece acesso ao AWS SSO para gerenciar contas de membros e aplicativos em nuvem da AWS organização

`AWSSSOMemberAccountAdministrator` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSSOMemberAccountAdministrator` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de junho de 2018, 20:45 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator`

Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListAccounts",
```

```
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy",
        "signin:CreateTrustedIdentityPropagationApplicationForConsole",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
```

```
      }
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSSOReadOnly

Descrição: Fornece acesso somente para leitura às configurações AWS de SSO.

`AWSSSOReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSSOReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de junho de 2018, 20:24 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOReadOnly`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListRoots",
```

```
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso:Search*",
        "sso-directory:DescribeDirectory",
        "access-analyzer:ValidatePolicy",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSSOServiceRolePolicy

Descrição: Concede permissões de AWS SSO para gerenciar AWS recursos, incluindo funções, políticas e SAML IdP em seu nome.

`AWSSSOServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 05 de dezembro de 2017, 18:36 UTC
- Horário editado: 11 de fevereiro de 2025, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

Versão da política

Versão da política: v18 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMRoleProvisioningActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription",
        "iam:UpdateAssumeRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:DeleteRolePermissionsBoundary"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMRoleReadActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMRoleCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ]
```

```
    },
    {
      "Sid" : "IAMSLRCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:DeleteRole",
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO"
      ]
    },
    {
      "Sid" : "IAMSAMLProviderCreationAction",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMSAMLProviderUpdateAction",
      "Effect" : "Allow",
      "Action" : [
        "iam:UpdateSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ]
    },
    {
      "Sid" : "IAMSAMLProviderCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSAMLProvider",
```

```
        "iam:GetSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowUnauthAppForDirectory",
      "Effect" : "Allow",
      "Action" : [
        "ds:UnauthorizeApplication"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeForDirectory",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeAndListOperationsOnIdentitySource",
      "Effect" : "Allow",
      "Action" : [
```

```
        "identitystore:DescribeUser",
        "identitystore:DescribeGroup",
        "identitystore:ListGroups",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDeleteSyncProfile",
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile"
      ],
      "Resource" : [
        "arn:aws:identity-sync:*:*:profile/*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSStepFunctionsConsoleFullAccess

Descrição: Uma política de acesso para fornecer um acesso user/role /etc ao AWS StepFunctions console. Para uma experiência completa do console, além dessa política, um usuário pode precisar da PassRole permissão iam: em outras funções do IAM que podem ser assumidas pelo serviço.

`AWSStepFunctionsConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSStepFunctionsConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de janeiro de 2017, 21:54 UTC
- Hora da edição: 12 de janeiro de 2017, 0:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/StatesExecutionRole*"
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:ListFunctions",
      "Resource" : "*"
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSStepFunctionsFullAccess

Descrição: uma política de acesso para fornecer um acesso user/role /etc à AWS StepFunctions API. Para ter acesso total, além dessa política, um usuário DEVE ter a PassRole permissão iam: em pelo menos uma função do IAM que possa ser assumida pelo serviço.

`AWSStepFunctionsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSStepFunctionsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de janeiro de 2017, 21:51 UTC
- Hora da edição: 11 de janeiro de 2017, 21:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSStepFunctionsReadOnlyAccess

Descrição: uma política de acesso para fornecer acesso somente para leitura user/role /etc ao AWS StepFunctions serviço.

`AWSStepFunctionsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSStepFunctionsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de janeiro de 2017, 21:46 UTC
- Hora da edição: 26 de abril de 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:ListActivities",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineForExecution",
        "states:ListExecutions",
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:DescribeActivity",
        "states:ListTagsForResource",
        "states:DescribeMapRun",
        "states:ListMapRuns",
        "states:DescribeStateMachineAlias",
        "states:ListStateMachineAliases",
        "states:ListStateMachineVersions",
        "states:ValidateStateMachineDefinition"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSStorageGatewayFullAccess

Descrição: Fornece acesso total ao AWS Storage Gateway por meio do Console de gerenciamento da AWS.

`AWSStorageGatewayFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSStorageGatewayFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 06 de setembro de 2022, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:*"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "fetchStorageGatewayParams",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSStorageGatewayReadOnlyAccess

Descrição: Fornece acesso ao AWS Storage Gateway por meio do Console de gerenciamento da AWS.

`AWSStorageGatewayReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSStorageGatewayReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 06 de setembro de 2022, 20:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:List*",
        "storagegateway:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "fetchStorageGatewayParams",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSStorageGatewayServiceRolePolicy

Descrição: Service-linked função usada pelo AWS Storage Gateway para permitir a integração de outros AWS serviços com o Storage Gateway.

`AWSStorageGatewayServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 17 de fevereiro de 2021, 19:03 UTC
- Hora da edição: 17 de fevereiro de 2021, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSupplyChainFederationAdminAccess

Descrição: AWSSupplyChainFederationAdminAccess fornece aos usuários federados da AWS Supply Chain acesso ao aplicativo AWS Supply Chain, incluindo as permissões necessárias para realizar ações dentro do aplicativo AWS Supply Chain. A política fornece permissões administrativas sobre usuários e grupos do IAM Identity Center e está vinculada a uma função criada pela AWS Supply Chain em seu nome. Você não deve anexar AWSSupplyChainFederationAdminAccess políticas a nenhuma outra entidade do IAM.

`AWSSupplyChainFederationAdminAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSupplyChainFederationAdminAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço

- Hora da criação: 01 de março de 2023, 18:54 UTC
- Horário editado: 14 de agosto de 2026, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSupplyChain",
      "Effect" : "Allow",
      "Action" : [
        "scn:*"
      ],
      "Resource" : [
        "arn:aws:scn:*:*:instance/*"
      ]
    },
    {
      "Sid" : "ChimeAppInstance",
      "Effect" : "Allow",
      "Action" : [
        "chime:BatchCreateChannelMembership",
        "chime:CreateAppInstanceUser",
        "chime:CreateChannel",
        "chime:CreateChannelMembership",
        "chime:CreateChannelModerator",
        "chime:Connect",
        "chime:DeleteChannelMembership",
        "chime:DeleteChannelModerator",
        "chime:DescribeChannelMembershipForAppInstanceUser",
```

```
        "chime:GetChannelMembershipPreferences",
        "chime:ListChannelMemberships",
        "chime:ListChannelMembershipsForAppInstanceUser",
        "chime:ListChannelMessages",
        "chime:ListChannelModerators",
        "chime:TagResource",
        "chime:PutChannelMembershipPreferences",
        "chime:SendChannelMessage",
        "chime:UpdateChannelReadMarker",
        "chime:UpdateAppInstanceUser"
      ],
      "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SCNInstanceId" : "*"
        }
      }
    },
    {
      "Sid" : "ChimeChannel",
      "Effect" : "Allow",
      "Action" : [
        "chime:DescribeChannel"
      ],
      "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
      ]
    },
    {
      "Sid" : "ChimeMessaging",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetMessagingSessionEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:ListDirectoryAssociations",
```

```
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso:ListApplicationAssignments",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:GetApplicationAssignmentConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BuilderIDCollaboration",
      "Effect" : "Allow",
      "Action" : [
        "builderid:CreateInvitation",
        "builderid:ListInvitations",
        "builderid:DeleteInvitation",
        "builderid:DisassociateCollaborator"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IdentityStoreCollaboration",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ReserveUser",
        "identitystore:DeleteUser"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AppflowConnectorProfile",
      "Effect" : "Allow",
      "Action" : [
        "appflow:CreateConnectorProfile",
        "appflow:UseConnectorProfile",
        "appflow:DeleteConnectorProfile",
```

```
        "appflow:UpdateConnectorProfile"
      ],
      "Resource" : [
        "arn:aws:appflow:*:*:connectorprofile/scn-*"
      ]
    },
    {
      "Sid" : "AppflowFlow",
      "Effect" : "Allow",
      "Action" : [
        "appflow:CreateFlow",
        "appflow:DeleteFlow",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:ListFlows",
        "appflow:StartFlow",
        "appflow:StopFlow",
        "appflow:UpdateFlow",
        "appflow:TagResource",
        "appflow:UntagResource"
      ],
      "Resource" : [
        "arn:aws:appflow:*:*:flow/scn-*"
      ]
    },
    {
      "Sid" : "S3ListAllBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ListSupplyChainBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-supply-chain-data-*"
      ]
```

```
    },
    {
      "Sid" : "S3ReadWriteObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-supply-chain-data-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "appflow!*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPutResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
```

```
          ]
        },
        "StringEqualsIgnoreCase" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appflow"
        }
      }
    },
    {
      "Sid" : "KMSListKeys",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSListGrants",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListGrants"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceTag/aws-supply-chain-access" : "true"
        }
      }
    },
    {
      "Sid" : "KMSCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
```

```
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringEquals" : {
          "aws:ResourceTag/aws-supply-chain-access" : "true"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSupportAccess

Descrição: Permite que os usuários acessem o AWS Support Centro.

`AWSSupportAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSupportAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:*",
        "support-console:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSupportAppFullAccess

Descrição: Fornece acesso total ao AWS Support aplicativo e a outros serviços necessários, como AWS Support cotas de serviço. Essa política inclui permissões para usar os serviços de suporte para que o usuário possa entrar em contato AWS Support para casos de suporte, alterar as cotas de serviço e criar as funções relevantes vinculadas ao serviço.

`AWSSupportAppFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSupportAppFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 22 de agosto de 2022, 16:53 UTC
- Hora da edição: 22 de agosto de 2022, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:RequestServiceQuotaIncrease",
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:DescribeSeverityLevels",
        "support:InitiateChatForCase",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSupportAppReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao AWS Support aplicativo.

`AWSSupportAppReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSupportAppReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 22 de agosto de 2022, 17:01 UTC
- Hora da edição: 22 de agosto de 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeCases",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSupportPlansFullAccess

Descrição: fornece acesso total aos planos de suporte.

`AWSSupportPlansFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSupportPlansFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de setembro de 2022, 18:19 UTC
- Horário editado: 24 de agosto de 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule",
        "supportplans:AcceptSupportAgreement",
        "supportplans:CancelSupportAgreement",
        "supportplans:CreateSupportAgreement",
        "supportplans:GetSupportAgreement",
        "supportplans:ListSupportAgreements",
        "supportplans:ListSupportAgreementRevisions",
        "supportplans:RejectSupportAgreement",
        "supportplans:UpdateSupportAgreement"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/supportplans.amazonaws.com/
AWSServiceRoleForSupportPlans",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "supportplans.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/supportplans.amazonaws.com/
AWSServiceRoleForSupportPlans"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSupportPlansReadOnlyAccess

Descrição: fornece acesso somente leitura aos planos de suporte.

`AWSSupportPlansReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSupportPlansReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de setembro de 2022, 18:08 UTC
- Horário editado: 24 de agosto de 2026, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
        "supportplans:GetSupportAgreement",
        "supportplans:ListSupportAgreements",
        "supportplans:ListSupportAgreementRevisions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSupportPlansServiceRolePolicy

Descrição: permite que AWS Support os Planos leiam e atualizem AWS os recursos usados para gerenciar o Plano de Suporte da sua conta em seu nome.

`AWSSupportPlansServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 31 de julho de 2026, 17:12 UTC
- Horário editado: 31 de julho de 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportPlansServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:AcceptSupportAgreement",
        "supportplans:CancelSupportAgreement",
        "supportplans:CreateSupportAgreement",
        "supportplans:GetSupportAgreement",
        "supportplans:ListSupportAgreements",
        "supportplans:ListSupportAgreementRevisions",
        "supportplans:RejectSupportAgreement",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:UpdateSupportAgreement",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSupportServiceRolePolicy

Descrição: Permite AWS Support acessar AWS recursos para fornecer serviços de cobrança, administrativos e de suporte.

`AWSSupportServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 19 de abril de 2018, 18:04 UTC
- Horário editado: 19 de agosto de 2026, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy`

Versão da política

Versão da política: v59 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "AWSSupportAPIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*:*:/domainnameaccessassociations",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
```

```
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "AWSSupportDeleteRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/support.amazonaws.com/
AWSServiceRoleForSupport"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup1",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:getAccessPreview",
        "access-analyzer:getAnalyzedResource",
        "access-analyzer:getAnalyzer",
        "access-analyzer:getArchiveRule",
        "access-analyzer:getFinding",
        "access-analyzer:getGeneratedPolicy",
        "access-analyzer:listAccessPreviewFindings",
        "access-analyzer:listAccessPreviews",
        "access-analyzer:listAnalyzedResources",
        "access-analyzer:listAnalyzers",
        "access-analyzer:listArchiveRules",
        "access-analyzer:listFindings",
        "access-analyzer:listPolicyGenerations",
```

```
        "account:getRegionOptStatus",
        "account:listRegions",
        "acm-pca:describeCertificateAuthority",
        "acm-pca:describeCertificateAuthorityAuditReport",
        "acm-pca:getCertificate",
        "acm-pca:getCertificateAuthorityCertificate",
        "acm-pca:getCertificateAuthorityCsr",
        "acm-pca:listCertificateAuthorities",
        "acm-pca:listTags",
        "acm:describeAcmeAccount",
        "acm:describeAcmeDomainValidation",
        "acm:describeAcmeEndpoint",
        "acm:describeAcmeExternalAccountBinding",
        "acm:describeCertificate",
        "acm:getAccountConfiguration",
        "acm:getCertificate",
        "acm:listAcmeAccounts",
        "acm:listAcmeDomainValidations",
        "acm:listAcmeEndpoints",
        "acm:listAcmeExternalAccountBindings",
        "acm:listCertificates",
        "acm:listTagsForCertificate",
        "acm:searchCertificates",
        "aidevops:describePrivateConnection",
        "aidevops:getAccountUsage",
        "aidevops:getAgentSpace",
        "aidevops:getAssociation",
        "aidevops:getBacklogTask",
        "aidevops:getOperatorApp",
        "aidevops:getRecommendation",
        "aidevops:getService",
        "aidevops:listAgentSpaces",
        "aidevops:listAssociations",
        "aidevops:listBacklogTasks",
        "aidevops:listChats",
        "aidevops:listExecutions",
        "aidevops:listGoals",
        "aidevops:listPrivateConnections",
        "aidevops:listRecommendations",
        "aidevops:listServices",
        "aidevops:listWebHooks",
        "aiops:getInvestigationGroup",
        "aiops:getInvestigationGroupPolicy",
        "aiops:listInvestigationGroups",
```

```
        "airflow-serverless:getTaskInstance",
        "airflow-serverless:getWorkflow",
        "airflow-serverless:getWorkflowRun",
        "airflow-serverless:listTaskInstances",
        "airflow-serverless:listWorkflowRuns",
        "airflow-serverless:listWorkflows",
        "airflow-serverless:listWorkflowVersions",
        "airflow:getEnvironment",
        "airflow:listEnvironments",
        "airflow:listTagsForResource",
        "amplify:getApp",
        "amplify:getBackendEnvironment",
        "amplify:getBranch",
        "amplify:getDomainAssociation",
        "amplify:getJob",
        "amplify:getWebhook",
        "amplify:listApps",
        "amplify:listBackendEnvironments",
        "amplify:listBranches",
        "amplify:listDomainAssociations",
        "amplify:listJobs",
        "amplify:listResourcesForWebACL",
        "amplify:listWebhooks",
        "amplifyuibuilder:exportComponents",
        "amplifyuibuilder:exportThemes",
        "apigateway:getPortal",
        "apigateway:getPortalProduct",
        "apigateway:getPortalProductSharingPolicy",
        "apigateway:getProductPage",
        "apigateway:getProductRestEndpointPage",
        "apigateway:getRoutingRule",
        "apigateway:listPortalProducts",
        "apigateway:listPortals",
        "apigateway:listProductPages",
        "apigateway:listProductRestEndpointPages",
        "apigateway:listRoutingRules",
        "aoss:batchGetCollection",
        "aoss:batchGetCollectionGroup",
        "aoss:batchGetEffectiveLifecyclePolicy",
        "aoss:batchGetLifecyclePolicy",
        "aoss:batchGetVpcEndpoint",
        "aoss:getAccessPolicy",
        "aoss:getAccountSettings",
        "aoss:getIndex",
```

```
        "aoss:getPoliciesStats",
        "aoss:getSecurityConfig",
        "aoss:getSecurityPolicy",
        "aoss:listAccessPolicies",
        "aoss:listCollectionGroups",
        "aoss:listCollections",
        "aoss:listLifecyclePolicies",
        "aoss:listSecurityConfigs",
        "aoss:listSecurityPolicies",
        "aoss:listTagsForResource",
        "aoss:listVpcEndpoints",
        "appconfig:getAccountSettings",
        "appconfig:getApplication",
        "appconfig:getConfigurationProfile",
        "appconfig:getDeployment",
        "appconfig:getDeploymentStrategy",
        "appconfig:getEnvironment",
        "appconfig:getExtension",
        "appconfig:getExtensionAssociation",
        "appconfig:getHostedConfigurationVersion",
        "appconfig:listApplications",
        "appconfig:listConfigurationProfiles",
        "appconfig:listDeployments",
        "appconfig:listDeploymentStrategies",
        "appconfig:listEnvironments",
        "appconfig:listExtensionAssociations",
        "appconfig:listExtensions",
        "appconfig:listHostedConfigurationVersions",
        "appflow:describeConnectorEntity",
        "appflow:describeConnectorProfiles",
        "appflow:describeConnectors",
        "appflow:describeFlow",
        "appflow:describeFlowExecutionRecords",
        "appflow:listConnectorEntities",
        "appflow:listFlows",
        "application-autoscaling:describeScalableTargets",
        "application-autoscaling:describeScalingActivities",
        "application-autoscaling:describeScalingPolicies",
        "application-autoscaling:describeScheduledActions",
        "application-signals:getService",
        "application-signals:getServiceLevelObjective",
        "application-signals:listServiceDependencies",
        "application-signals:listServiceDependents",
        "application-signals:listServiceLevelObjectives",
```

```
        "application-signals:listServiceOperations",
        "application-signals:listServices",
        "applicationinsights:describeApplication",
        "applicationinsights:describeComponent",
        "applicationinsights:describeComponentConfiguration",
        "applicationinsights:describeComponentConfigurationRecommendation",
        "applicationinsights:describeLogPattern",
        "applicationinsights:describeObservation",
        "applicationinsights:describeProblem",
        "applicationinsights:describeProblemObservations",
        "applicationinsights:listApplications",
        "applicationinsights:listComponents",
        "applicationinsights:listConfigurationHistory",
        "applicationinsights:listLogPatterns",
        "applicationinsights:listLogPatternSets",
        "applicationinsights:listProblems",
        "appmesh:describeGatewayRoute",
        "appmesh:describeMesh",
        "appmesh:describeRoute",
        "appmesh:describeVirtualGateway",
        "appmesh:describeVirtualNode",
        "appmesh:describeVirtualRouter",
        "appmesh:describeVirtualService",
        "appmesh:listGatewayRoutes",
        "appmesh:listMeshes",
        "appmesh:listRoutes",
        "appmesh:listTagsForResource",
        "appmesh:listVirtualGateways",
        "appmesh:listVirtualNodes",
        "appmesh:listVirtualRouters",
        "appmesh:listVirtualServices",
        "apprunner:describeAutoScalingConfiguration",
        "apprunner:describeCustomDomains",
        "apprunner:describeObservabilityConfiguration",
        "apprunner:describeOperation",
        "apprunner:describeService",
        "apprunner:describeVpcConnector",
        "apprunner:describeVpcIngressConnection",
        "apprunner:listAutoScalingConfigurations",
        "apprunner:listConnections",
        "apprunner:listObservabilityConfigurations",
        "apprunner:listOperations",
        "apprunner:listAssociatedServicesForWebAcl",
        "apprunner:listServices",
```

```
        "apprunner:listTagsForResource",
        "apprunner:listVpcConnectors",
        "apprunner:listVpcIngressConnections",
        "appstream:describeAppBlockBuilderAppBlockAssociations",
        "appstream:describeAppBlockBuilders",
        "appstream:describeAppBlocks",
        "appstream:describeApplicationFleetAssociations",
        "appstream:describeApplications",
        "appstream:describeDirectoryConfigs",
        "appstream:describeEntitlements",
        "appstream:describeFleets",
        "appstream:describeImageBuilders",
        "appstream:describeImagePermissions",
        "appstream:describeImages",
        "appstream:describeSessions",
        "appstream:describeStacks",
        "appstream:describeUsageReportSubscriptions",
        "appstream:describeUsers",
        "appstream:describeUserStackAssociations",
        "appstream:listAssociatedFleets",
        "appstream:listAssociatedStacks",
        "appstream:listEntitledApplications",
        "appstream:listTagsForResource",
        "appsync:evaluateCode",
        "appsync:evaluateMappingTemplate",
        "appsync:getApi",
        "appsync:getApiAssociation",
        "appsync:getApiCache",
        "appsync:getChannelNamespace",
        "appsync:getDataSource",
        "appsync:getDataSourceIntrospection",
        "appsync:getDomainName",
        "appsync:getFunction",
        "appsync:getGraphqlApi",
        "appsync:getGraphqlApiEnvironmentVariables",
        "appsync:getIntrospectionSchema",
        "appsync:getResolver",
        "appsync:getSchemaCreationStatus",
        "appsync:getSourceApiAssociation",
        "appsync:getType",
        "appsync:listApis",
        "appsync:listChannelNamespaces",
        "appsync:listDataSources",
        "appsync:listDomainNames",
```

```
        "appsync:listFunctions",
        "appsync:listGraphqlApis",
        "appsync:listResolvers",
        "appsync:listResolversByFunction",
        "appsync:listSourceApiAssociations",
        "appsync:listTypes",
        "appsync:listTypesByAssociation",
        "aps:describeAlertManagerDefinition",
        "aps:describeRuleGroupsNamespace",
        "aps:describeScraper",
        "aps:describeWorkspace",
        "aps:listRuleGroupsNamespaces",
        "aps:listScrapers",
        "aps:listWorkspaces",
        "arc-zonal-shift:getAutoshiftObserverNotificationStatus",
        "arc-zonal-shift:getManagedResource",
        "arc-zonal-shift:listAutoshifts",
        "arc-zonal-shift:listManagedResources",
        "arc-zonal-shift:listZonalShifts",
        "athena:batchGetNamedQuery",
        "athena:batchGetQueryExecution",
        "athena:getCalculationExecution",
        "athena:getCalculationExecutionStatus",
        "athena:getCapacityAssignmentConfiguration",
        "athena:getCapacityReservation",
        "athena:getDataCatalog",
        "athena:getNamedQuery",
        "athena:getNotebookMetadata",
        "athena:getQueryExecution",
        "athena:getQueryRuntimeStatistics",
        "athena:getSession",
        "athena:getSessionStatus",
        "athena:getWorkGroup",
        "athena:listApplicationDPUSizes",
        "athena:listCalculationExecutions",
        "athena:listCapacityReservations",
        "athena:listDataCatalogs",
        "athena:listEngineVersions",
        "athena:listExecutors",
        "athena:listNamedQueries",
        "athena:listNotebookMetadata",
        "athena:listNotebookSessions",
        "athena:listQueryExecutions",
        "athena:listSessions",
```

```
        "athena:listTagsForResource",
        "athena:listWorkGroups",
        "auditmanager:getAccountStatus",
        "auditmanager:getDelegations",
        "auditmanager:listAssessmentFrameworks",
        "auditmanager:listAssessmentReports",
        "auditmanager:listAssessments",
        "auditmanager:listControls",
        "auditmanager:listKeywordsForDataSource",
        "auditmanager:listNotifications",
        "autoscaling-plans:describeScalingPlanResources",
        "autoscaling-plans:describeScalingPlans",
        "autoscaling-plans:getScalingPlanResourceForecastData",
        "autoscaling:describeAccountLimits",
        "autoscaling:describeAdjustmentTypes",
        "autoscaling:describeAutoScalingGroups",
        "autoscaling:describeAutoScalingInstances",
        "autoscaling:describeAutoScalingNotificationTypes",
        "autoscaling:describeInstanceRefreshes",
        "autoscaling:describeLaunchConfigurations",
        "autoscaling:describeLifecycleHooks",
        "autoscaling:describeLifecycleHookTypes",
        "autoscaling:describeLoadBalancers",
        "autoscaling:describeLoadBalancerTargetGroups",
        "autoscaling:describeMetricCollectionTypes",
        "autoscaling:describeNotificationConfigurations",
        "autoscaling:describePolicies",
        "autoscaling:describeScalingActivities",
        "autoscaling:describeScalingProcessTypes",
        "autoscaling:describeScheduledActions",
        "autoscaling:describeTags",
        "autoscaling:describeTerminationPolicyTypes",
        "autoscaling:describeTrafficSources",
        "autoscaling:describeWarmPool",
        "aws-marketplace:describeAgreement",
        "aws-marketplace:describeEntity",
        "aws-marketplace:listEntities",
        "aws-marketplace:searchAgreements",
        "backup-gateway:getBandwidthRateLimitSchedule",
        "backup-gateway:getGateway",
        "backup-gateway:getHypervisor",
        "backup-gateway:getHypervisorPropertyMappings",
        "backup-gateway:getVirtualMachine",
        "backup-gateway:listGateways",
```

```
        "backup-gateway:listHypervisors",
        "backup-gateway:listVirtualMachines",
        "backup-gateway:listTagsForResource",
        "backup-search:getSearchJob",
        "backup-search:getSearchResultExportJob",
        "backup-search:listSearchJobBackups",
        "backup-search:listSearchJobs",
        "backup-search:listSearchResultExportJobs",
        "backup-search:listTagsForResource",
        "backup:describeBackupAccessPoint",
        "backup:describeScanJob",
        "backup:describeBackupJob",
        "backup:describeBackupVault",
        "backup:describeCopyJob",
        "backup:describeFramework",
        "backup:describeGlobalSettings",
        "backup:describeProtectedResource",
        "backup:describeRecoveryPoint",
        "backup:describeRegionSettings",
        "backup:describeReportJob",
        "backup:describeReportPlan",
        "backup:describeRestoreJob",
        "backup:getBackupPlan",
        "backup:getBackupPlanFromJSON",
        "backup:getBackupPlanFromTemplate",
        "backup:getBackupSelection",
        "backup:getBackupVaultAccessPolicy",
        "backup:getBackupVaultNotifications",
        "backup:getLegalHold",
        "backup:getRecoveryPointRestoreMetadata",
        "backup:getRecoveryPointIndexDetails",
        "backup:getRestoreJobMetadata",
        "backup:getRestoreTestingInferredMetadata",
        "backup:getRestoreTestingPlan",
        "backup:getRestoreTestingSelection",
        "backup:getSupportedResourceTypes",
        "backup:getTieringConfiguration",
        "backup:listBackupJobs",
        "backup:listBackupJobSummaries",
        "backup:listBackupPlans",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "backup:listBackupSelections",
        "backup:listBackupVaults",
```

```
        "backup:listCopyJobs",
        "backup:listCopyJobSummaries",
        "backup:listFrameworks",
        "backup:listIndexedRecoveryPoints",
        "backup:listLegalHolds",
        "backup:listProtectedResources",
        "backup:listProtectedResourcesByBackupVault",
        "backup:listRecoveryPointsByBackupVault",
        "backup:listRecoveryPointsByLegalHold",
        "backup:listRecoveryPointsByResource",
        "backup:listReportJobs",
        "backup:listReportPlans",
        "backup:listRestoreAccessBackupVaults",
        "backup:listRestoreJobs",
        "backup:listRestoreJobsByProtectedResource",
        "backup:listRestoreJobSummaries",
        "backup:listRestoreTestingPlans",
        "backup:listRestoreTestingSelections",
        "backup:listScanJobSummaries",
        "backup:listScanJobs",
        "backup:listTags",
        "backup:listTieringConfigurations",
        "batch:describeComputeEnvironments",
        "batch:describeConsumableResource",
        "batch:describeJobDefinitions",
        "batch:describeJobQueues",
        "batch:describeJobs",
        "batch:describeSchedulingPolicies",
        "batch:describeServiceEnvironments",
        "batch:describeServiceJob",
        "batch:getJobQueueSnapshot",
        "batch:listConsumableResources",
        "batch:listJobs",
        "batch:listJobsByConsumableResource",
        "batch:listSchedulingPolicies",
        "batch:listServiceJobs",
        "batch:listTagsForResource",
        "bedrock:exportAutomatedReasoningPolicyVersion",
        "bedrock:getAgent",
        "bedrock:getAgentActionGroup",
        "bedrock:getAgentAlias",
        "bedrock:getAgentKnowledgeBase",
        "bedrock:getAgentMemory",
        "bedrock:getAgentVersion",
```

```
        "bedrock:getAsyncInvoke",
        "bedrock:getAutomatedReasoningPolicy",
        "bedrock:getAutomatedReasoningPolicyAnnotations",
        "bedrock:getAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:getAutomatedReasoningPolicyBuildWorkflowResultAssets",
        "bedrock:getAutomatedReasoningPolicyNextScenario",
        "bedrock:getAutomatedReasoningPolicyTestCase",
        "bedrock:getAutomatedReasoningPolicyTestResult",
        "bedrock:getBlueprint",
        "bedrock:getCustomModel",
        "bedrock:getCustomModelDeployment",
        "bedrock:getDataAutomationProject",
        "bedrock:getDataAutomationStatus",
        "bedrock:getDataSource",
        "bedrock:getEvaluationJob",
        "bedrock:getExecutionFlowSnapshot",
        "bedrock:getFlow",
        "bedrock:getFlowAlias",
        "bedrock:getFlowExecution",
        "bedrock:getFlowVersion",
        "bedrock:getFoundationModel",
        "bedrock:getFoundationModelAvailability",
        "bedrock:getGuardrail",
        "bedrock:getImportedModel",
        "bedrock:getInferenceProfile",
        "bedrock:getIngestionJob",
        "bedrock:getInvocationStep",
        "bedrock:getKnowledgeBase",
        "bedrock:getMarketplaceModelEndpoint",
        "bedrock:getModelCopyJob",
        "bedrock:getModelCustomizationJob",
        "bedrock:getModelImportJob",
        "bedrock:getModelInvocationJob",
        "bedrock:getModelInvocationLoggingConfiguration",
        "bedrock:getPrompt",
        "bedrock:getPromptRouter",
        "bedrock:getProvisionedModelThroughput",
        "bedrock:getSession",
        "bedrock:getUseCaseForModelAccess",
        "bedrock:listAgentActionGroups",
        "bedrock:listAgentAliases",
        "bedrock:listAgentKnowledgeBases",
        "bedrock:listAgents",
        "bedrock:listAgentVersions",
```

```
        "bedrock:listAsyncInvokes",
        "bedrock:listAutomatedReasoningPolicies",
        "bedrock:listAutomatedReasoningPolicyBuildWorkflows",
        "bedrock:listAutomatedReasoningPolicyTestCases",
        "bedrock:listAutomatedReasoningPolicyTestResults",
        "bedrock:listBlueprints",
        "bedrock:listCustomModelDeployments",
        "bedrock:listCustomModels",
        "bedrock:listDataAutomationProjects",
        "bedrock:listDataSources",
        "bedrock:listEnforcedGuardrailsConfiguration",
        "bedrock:listEvaluationJobs",
        "bedrock:listFlowAliases",
        "bedrock:listFlowExecutionEvents",
        "bedrock:listFlowExecutions",
        "bedrock:listFlows",
        "bedrock:listFlowVersions",
        "bedrock:listFoundationModelAgreementOffers",
        "bedrock:listFoundationModels",
        "bedrock:listGuardrails",
        "bedrock:listImportedModels",
        "bedrock:listInferenceProfiles",
        "bedrock:listIngestionJobs",
        "bedrock:listInvocationSteps",
        "bedrock:listKnowledgeBases",
        "bedrock:listMarketplaceModelEndpoints",
        "bedrock:listModelCopyJobs",
        "bedrock:listModelCustomizationJobs",
        "bedrock:listModelImportJobs",
        "bedrock:listModelInvocationJobs",
        "bedrock:listPromptRouters",
        "bedrock:listPrompts",
        "bedrock:listProvisionedModelThroughputs",
        "bedrock:listSessions",
        "bedrock-agentcore:getAgentCard",
        "bedrock-agentcore:getAgentRuntime",
        "bedrock-agentcore:getAgentRuntimeEndpoint",
        "bedrock-agentcore:getApiKeyCredentialProvider",
        "bedrock-agentcore:getBrowser",
        "bedrock-agentcore:getBrowserProfile",
        "bedrock-agentcore:getBrowserSession",
        "bedrock-agentcore:getCodeInterpreter",
        "bedrock-agentcore:getCodeInterpreterSession",
        "bedrock-agentcore:getConfigurationBundle",
```

```
        "bedrock-agentcore:getConfigurationBundleVersion",
        "bedrock-agentcore:getEvaluator",
        "bedrock-agentcore:getEvent",
        "bedrock-agentcore:getGateway",
        "bedrock-agentcore:getGatewayRule",
        "bedrock-agentcore:getGatewayTarget",
        "bedrock-agentcore:getHarness",
        "bedrock-agentcore:getMemory",
        "bedrock-agentcore:getMemoryRecord",
        "bedrock-agentcore:getOauth2CredentialProvider",
        "bedrock-agentcore:getOnlineEvaluationConfig",
        "bedrock-agentcore:getPaymentConnector",
        "bedrock-agentcore:getPaymentCredentialProvider",
        "bedrock-agentcore:getPaymentManager",
        "bedrock-agentcore:getPolicy",
        "bedrock-agentcore:getPolicyEngine",
        "bedrock-agentcore:getPolicyEngineSummary",
        "bedrock-agentcore:getPolicyGeneration",
        "bedrock-agentcore:getPolicyGenerationSummary",
        "bedrock-agentcore:getPolicySummary",
        "bedrock-agentcore:getRegistry",
        "bedrock-agentcore:getRegistryRecord",
        "bedrock-agentcore:getResourcePolicy",
        "bedrock-agentcore:getTokenVault",
        "bedrock-agentcore:getWorkloadIdentity",
        "bedrock-agentcore:listActors",
        "bedrock-agentcore:listAgentRuntimeEndpoints",
        "bedrock-agentcore:listAgentRuntimeVersions",
        "bedrock-agentcore:listAgentRuntimes",
        "bedrock-agentcore:listApiKeyCredentialProviders",
        "bedrock-agentcore:listBrowserProfiles",
        "bedrock-agentcore:listBrowserSessions",
        "bedrock-agentcore:listBrowsers",
        "bedrock-agentcore:listCodeInterpreterSessions",
        "bedrock-agentcore:listCodeInterpreters",
        "bedrock-agentcore:listConfigurationBundles",
        "bedrock-agentcore:listConfigurationBundleVersions",
        "bedrock-agentcore:listEvaluators",
        "bedrock-agentcore:listEvents",
        "bedrock-agentcore:listGatewayRules",
        "bedrock-agentcore:listGatewayTargets",
        "bedrock-agentcore:listGateways",
        "bedrock-agentcore:listHarnesses",
        "bedrock-agentcore:listMemories",
```

```
        "bedrock-agentcore:listMemoryExtractionJobs",
        "bedrock-agentcore:listMemoryRecords",
        "bedrock-agentcore:listOauth2CredentialProviders",
        "bedrock-agentcore:listOnlineEvaluationConfigs",
        "bedrock-agentcore:listPaymentConnectors",
        "bedrock-agentcore:listPaymentCredentialProviders",
        "bedrock-agentcore:listPaymentManagers",
        "bedrock-agentcore:listPolicies",
        "bedrock-agentcore:listPolicyEngines",
        "bedrock-agentcore:listPolicyEngineSummaries",
        "bedrock-agentcore:listPolicyGenerationAssets",
        "bedrock-agentcore:listPolicyGenerations",
        "bedrock-agentcore:listPolicyGenerationSummaries",
        "bedrock-agentcore:listPolicySummaries",
        "bedrock-agentcore:listRegistries",
        "bedrock-agentcore:listRegistryRecords",
        "bedrock-agentcore:listSessions",
        "bedrock-agentcore:listWorkloadIdentities",
        "braket:getDevice",
        "braket:getJob",
        "braket:getQuantumTask",
        "braket:getServiceLinkedRoleStatus",
        "braket:getUserAgreementStatus",
        "braket:searchDevices",
        "braket:searchJobs",
        "braket:searchQuantumTasks",
        "braket:searchSpendingLimits",
        "budgets:viewBudget",
        "ce:getCostAndUsage",
        "ce:getCostAndUsageWithResources",
        "ce:getCostForecast",
        "ce:getDimensionValues",
        "ce:getReservationCoverage",
        "ce:getReservationPurchaseRecommendation",
        "ce:getReservationUtilization",
        "ce:getRightsizingRecommendation",
        "ce:getSavingsPlansCoverage",
        "ce:getSavingsPlansPurchaseRecommendation",
        "ce:getSavingsPlansUtilization",
        "ce:getSavingsPlansUtilizationDetails",
        "ce:getTags",
        "chatbot:describeChimeWebhookConfigurations",
        "chatbot:describeSlackChannelConfigurations",
        "chatbot:describeSlackUserIdentities",
```

```
        "chatbot:describeSlackWorkspaces",
        "chatbot:getMicrosoftTeamsChannelConfiguration",
        "chatbot:listMicrosoftTeamsChannelConfigurations",
        "chatbot:listMicrosoftTeamsConfiguredTeams",
        "chatbot:listMicrosoftTeamsUserIdentities",
        "chime:describeAppInstance",
        "chime:getAttendee",
        "chime:getGlobalSettings",
        "chime:getMediaCapturePipeline",
        "chime:getMediaPipeline",
        "chime:getMeeting",
        "chime:getProxySession",
        "chime:getSipMediaApplication",
        "chime:getSipRule",
        "chime:getVoiceConnector",
        "chime:getVoiceConnectorGroup",
        "chime:getVoiceConnectorLoggingConfiguration",
        "chime:listAppInstances",
        "chime:listAttendees",
        "chime:listChannelBans",
        "chime:listChannels",
        "chime:listChannelsModeratedByAppInstanceUser",
        "chime:listMediaCapturePipelines",
        "chime:listMediaPipelines",
        "chime:listMeetings",
        "chime:listSipMediaApplications",
        "chime:listSipRules",
        "chime:listVoiceConnectorGroups",
        "chime:listVoiceConnectors",
        "cleanrooms:batchGetCollaborationAnalysisTemplate",
        "cleanrooms:batchGetSchema",
        "cleanrooms:getAnalysisTemplate",
        "cleanrooms:getCollaboration",
        "cleanrooms:getCollaborationAnalysisTemplate",
        "cleanrooms:getCollaborationConfiguredAudienceModelAssociation",
        "cleanrooms:getCollaborationPrivacyBudgetTemplate",
        "cleanrooms:getConfiguredTable",
        "cleanrooms:getConfiguredTableAnalysisRule",
        "cleanrooms:getConfiguredTableAssociation",
        "cleanrooms:getConfiguredAudienceModelAssociation",
        "cleanrooms:getMembership",
        "cleanrooms:getPrivacyBudgetTemplate",
        "cleanrooms:getSchema",
        "cleanrooms:getSchemaAnalysisRule",
```

```
        "cleanrooms:listAnalysisTemplates",
        "cleanrooms:listCollaborationAnalysisTemplates",
        "cleanrooms:listCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:listCollaborationPrivacyBudgetTemplates",
        "cleanrooms:listCollaborationPrivacyBudgets",
        "cleanrooms:listCollaborations",
        "cleanrooms:listConfiguredAudienceModelAssociations",
        "cleanrooms:listConfiguredTableAssociations",
        "cleanrooms:listConfiguredTables",
        "cleanrooms:listMembers",
        "cleanrooms:listMemberships",
        "cleanrooms:listPrivacyBudgetTemplates",
        "cleanrooms:listPrivacyBudgets",
        "cleanrooms:listProtectedQueries",
        "cleanrooms:listSchemas",
        "cleanrooms:previewPrivacyImpact",
        "cloud9:describeEnvironmentMemberships",
        "cloud9:describeEnvironments",
        "cloud9:listEnvironments",
        "clouddirectory:getDirectory",
        "clouddirectory:listDirectories",
        "cloudformation:batchDescribeTypeConfigurations",
        "cloudformation:describeAccountLimits",
        "cloudformation:describeChangeSet",
        "cloudformation:describeChangeSetHooks",
        "cloudformation:describeEvents",
        "cloudformation:describePublisher",
        "cloudformation:describeStackDriftDetectionStatus",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
        "cloudformation:describeStackResource",
        "cloudformation:describeStackResourceDrifts",
        "cloudformation:describeStackResources",
        "cloudformation:describeStacks",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
        "cloudformation:estimateTemplateCost",
        "cloudformation:getResource",
        "cloudformation:getStackPolicy",
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
```

```
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listResources",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
        "cloudformation:listStacks",
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
        "cloudformation:listStackSets",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypes",
        "cloudformation:listTypeVersions",
        "cloudfront:describeConnectionFunction",
        "cloudfront:describeFunction",
        "cloudfront:describeKeyValueStore",
        "cloudfront:getAnycastIpList",
        "cloudfront:getCachePolicy",
        "cloudfront:getCachePolicyConfig",
        "cloudfront:getCloudFrontOriginAccessIdentity",
        "cloudfront:getCloudFrontOriginAccessIdentityConfig",
        "cloudfront:getConnectionFunction",
        "cloudfront:getConnectionGroup",
        "cloudfront:getConnectionGroupByRoutingEndpoint",
        "cloudfront:getContinuousDeploymentPolicy",
        "cloudfront:getContinuousDeploymentPolicyConfig",
        "cloudfront:getDistribution",
        "cloudfront:getDistributionConfig",
        "cloudfront:getDistributionTenant",
        "cloudfront:getDistributionTenantByDomain",
        "cloudfront:getInvalidation",
        "cloudfront:getInvalidationForDistributionTenant",
        "cloudfront:getKeyGroup",
        "cloudfront:getKeyGroupConfig",
        "cloudfront:getManagedCertificateDetails",
        "cloudfront:getMonitoringSubscription",
        "cloudfront:getOriginAccessControl",
        "cloudfront:getOriginAccessControlConfig",
        "cloudfront:getOriginRequestPolicy",
        "cloudfront:getOriginRequestPolicyConfig",
        "cloudfront:getPublicKey",
        "cloudfront:getPublicKeyConfig",
        "cloudfront:getRealtimeLogConfig",
        "cloudfront:getResourcePolicy",
        "cloudfront:getResponseHeadersPolicy",
```

```
        "cloudfront:getResponseHeadersPolicyConfig",
        "cloudfront:getStreamingDistribution",
        "cloudfront:getStreamingDistributionConfig",
        "cloudfront:getTrustStore",
        "cloudfront:getVpcOrigin",
        "cloudfront:listAnycastIpLists",
        "cloudfront:listCachePolicies",
        "cloudfront:listCloudFrontOriginAccessIdentities",
        "cloudfront:listConnectionFunctions",
        "cloudfront:listConnectionGroups",
        "cloudfront:listConflictingAliases",
        "cloudfront:listContinuousDeploymentPolicies",
        "cloudfront:listDistributions",
        "cloudfront:listDistributionsByAnycastIpListId",
        "cloudfront:listDistributionsByCachePolicyId",
        "cloudfront:listDistributionsByConnectionFunction",
        "cloudfront:listDistributionsByConnectionMode",
        "cloudfront:listDistributionsByKeyGroup",
        "cloudfront:listDistributionsByOriginRequestPolicyId",
        "cloudfront:listDistributionsByRealtimeLogConfig",
        "cloudfront:listDistributionsByResponseHeadersPolicyId",
        "cloudfront:listDistributionsByTrustStore",
        "cloudfront:listDistributionsByVpcOriginId",
        "cloudfront:listDistributionsByWebACLId",
        "cloudfront:listDistributionTenants",
        "cloudfront:listDistributionTenantsByCustomization",
        "cloudfront:listDomainConflicts",
        "cloudfront:listFunctions",
        "cloudfront:listInvalidations",
        "cloudfront:listInvalidationsForDistributionTenant",
        "cloudfront:listKeyGroups",
        "cloudfront:listKeyValueStores",
        "cloudfront:listOriginAccessControls",
        "cloudfront:listOriginRequestPolicies",
        "cloudfront:listPublicKeys",
        "cloudfront:listRealtimeLogConfigs",
        "cloudfront:listResponseHeadersPolicies",
        "cloudfront:listStreamingDistributions",
        "cloudfront:listTagsForResource",
        "cloudfront:listTrustStores",
        "cloudfront:listVpcOrigins",
        "cloudhsm:describeBackups",
        "cloudhsm:describeClusters",
        "cloudsearch:describeAnalysisSchemes",
```

```
        "cloudsearch:describeAvailabilityOptions",
        "cloudsearch:describeDomains",
        "cloudsearch:describeExpressions",
        "cloudsearch:describeIndexFields",
        "cloudsearch:describeScalingParameters",
        "cloudsearch:describeServiceAccessPolicies",
        "cloudsearch:describeSuggesters",
        "cloudsearch:listDomainNames",
        "cloudtrail:describeTrails",
        "cloudtrail:getEventSelectors",
        "cloudtrail:getInsightSelectors",
        "cloudtrail:getTrail",
        "cloudtrail:getTrailStatus",
        "cloudtrail:listEventDataStores",
        "cloudtrail:listPublicKeys",
        "cloudtrail:listTags",
        "cloudtrail:listTrails",
        "cloudtrail:lookupEvents",
        "cloudwatch:describeAlarmHistory",
        "cloudwatch:describeAlarms",
        "cloudwatch:describeAlarmsForMetric",
        "cloudwatch:describeAnomalyDetectors",
        "cloudwatch:describeInsightRules",
        "cloudwatch:getDashboard",
        "cloudwatch:getInsightRuleReport",
        "cloudwatch:getMetricData",
        "cloudwatch:getMetricStatistics",
        "cloudwatch:getMetricStream",
        "cloudWatch:getMetricWidgetImage",
        "cloudwatch:listDashboards",
        "cloudwatch:listManagedInsightRules",
        "cloudwatch:listMetrics",
        "cloudwatch:listMetricStreams",
        "cloudwatch:getAlarmMuteRule",
        "cloudwatch:listAlarmMuteRules",
        "codeartifact:describeDomain",
        "codeartifact:describePackageVersion",
        "codeartifact:describeRepository",
        "codeartifact:getDomainPermissionsPolicy",
        "codeartifact:getRepositoryEndpoint",
        "codeartifact:getRepositoryPermissionsPolicy",
        "codeartifact:listDomains",
        "codeartifact:listPackages",
        "codeartifact:listPackageVersionAssets",
```

```
        "codeartifact:listPackageVersions",
        "codeartifact:listRepositories",
        "codeartifact:listRepositoriesInDomain",
        "codebuild:batchGetBuildBatches",
        "codebuild:batchGetBuilds",
        "codebuild:batchGetFleets",
        "codebuild:batchGetProjects",
        "codebuild:listBuildBatches",
        "codebuild:listBuildBatchesForProject",
        "codebuild:listBuilds",
        "codebuild:listBuildsForProject",
        "codebuild:listCuratedEnvironmentImages",
        "codebuild:listFleets",
        "codebuild:listProjects",
        "codebuild:listSourceCredentials",
        "codecommit:batchGetRepositories",
        "codecommit:getBranch",
        "codecommit:getRepository",
        "codecommit:getRepositoryTriggers",
        "codecommit:listBranches",
        "codecommit:listRepositories",
        "codeconnections:getConnection",
        "codeconnections:getHost",
        "codeconnections:getRepositoryLink",
        "codeconnections:getRepositorySyncStatus",
        "codeconnections:getResourceSyncStatus",
        "codeconnections:getSyncBlockerSummary",
        "codeconnections:getSyncConfiguration",
        "codeconnections:listConnections",
        "codeconnections:listHosts",
        "codeconnections:listRepositoryLinks",
        "codeconnections:listRepositorySyncDefinitions",
        "codeconnections:listSyncConfigurations",
        "codedeploy:batchGetApplicationRevisions",
        "codedeploy:batchGetApplications",
        "codedeploy:batchGetDeploymentGroups",
        "codedeploy:batchGetDeploymentInstances",
        "codedeploy:batchGetDeployments",
        "codedeploy:batchGetDeploymentTargets",
        "codedeploy:batchGetOnPremisesInstances",
        "codedeploy:getApplication",
        "codedeploy:getApplicationRevision",
        "codedeploy:getDeployment",
        "codedeploy:getDeploymentConfig",
```

```
        "codedeploy:getDeploymentGroup",
        "codedeploy:getDeploymentInstance",
        "codedeploy:getDeploymentTarget",
        "codedeploy:getOnPremisesInstance",
        "codedeploy:listApplicationRevisions",
        "codedeploy:listApplications",
        "codedeploy:listDeploymentConfigs",
        "codedeploy:listDeploymentGroups",
        "codedeploy:listDeploymentInstances",
        "codedeploy:listDeployments",
        "codedeploy:listDeploymentTargets",
        "codedeploy:listGitHubAccountTokenNames",
        "codedeploy:listOnPremisesInstances",
        "codepipeline:getJobDetails",
        "codepipeline:getPipeline",
        "codepipeline:getPipelineExecution",
        "codepipeline:getPipelineState",
        "codepipeline:listActionExecutions",
        "codepipeline:listActionTypes",
        "codepipeline:listPipelineExecutions",
        "codepipeline:listPipelines",
        "codepipeline:listRuleExecutions",
        "codepipeline:listWebhooks",
        "codestar-connections:getConnection",
        "codestar-connections:getHost",
        "codestar-connections:listConnections",
        "codestar-connections:listHosts",
        "codestar:describeProject",
        "codestar:listProjects",
        "codestar:listResources",
        "codestar:listTeamMembers",
        "codestar:listUserProfiles",
        "cognito-identity:describeIdentity",
        "cognito-identity:describeIdentityPool",
        "cognito-identity:getIdentityPoolAnalytics",
        "cognito-identity:getIdentityPoolDailyAnalytics",
        "cognito-identity:getIdentityPoolRoles",
        "cognito-identity:getIdentityProviderDailyAnalytics",
        "cognito-identity:listIdentities",
        "cognito-identity:listIdentityPools",
        "cognito-identity:lookupDeveloperIdentity",
        "cognito-idp:describeIdentityProvider",
        "cognito-idp:describeManagedLoginBranding",
        "cognito-idp:describeManagedLoginBrandingByClient",
```

```
        "cognito-idp:describeResourceServer",
        "cognito-idp:describeRiskConfiguration",
        "cognito-idp:describeUserImportJob",
        "cognito-idp:describeUserPool",
        "cognito-idp:describeUserPoolClient",
        "cognito-idp:describeUserPoolDomain",
        "cognito-idp:getCSVHeader",
        "cognito-idp:getGroup",
        "cognito-idp:getLogDeliveryConfiguration",
        "cognito-idp:getUICustomization",
        "cognito-idp:getUserPoolMfaConfig",
        "cognito-idp:getWebACLForResource",
        "cognito-idp:listGroups",
        "cognito-idp:listIdentityProviders",
        "cognito-idp:listResourceServers",
        "cognito-idp:listResourcesForWebACL",
        "cognito-idp:listUserImportJobs",
        "cognito-idp:listUserPoolClients",
        "cognito-idp:listUserPools",
        "cognito-sync:describeDataset",
        "cognito-sync:describeIdentityPoolUsage",
        "cognito-sync:describeIdentityUsage",
        "cognito-sync:getCognitoEvents",
        "cognito-sync:getIdentityPoolConfiguration",
        "cognito-sync:listDatasets",
        "cognito-sync:listIdentityPoolUsage",
        "comprehend:describeDocumentClassificationJob",
        "comprehend:describeDocumentClassifier",
        "comprehend:describeDominantLanguageDetectionJob",
        "comprehend:describeEndpoint",
        "comprehend:describeEntitiesDetectionJob",
        "comprehend:describeEntityRecognizer",
        "comprehend:describeEventsDetectionJob",
        "comprehend:describeFlywheel",
        "comprehend:describeFlywheelIteration",
        "comprehend:describeKeyPhrasesDetectionJob",
        "comprehend:describePiiEntitiesDetectionJob",
        "comprehend:describeSentimentDetectionJob",
        "comprehend:describeTargetedSentimentDetectionJob",
        "comprehend:describeTopicsDetectionJob",
        "comprehend:listDocumentClassificationJobs",
        "comprehend:listDocumentClassifiers",
        "comprehend:listDominantLanguageDetectionJobs",
        "comprehend:listEndpoints",
```

```
        "comprehend:listEntitiesDetectionJobs",
        "comprehend:listEntityRecognizers",
        "comprehend:listEventsDetectionJobs",
        "comprehend:listFlywheelIterationHistory",
        "comprehend:listFlywheels",
        "comprehend:listKeyPhrasesDetectionJobs",
        "comprehend:listPiiEntitiesDetectionJobs",
        "comprehend:listSentimentDetectionJobs",
        "comprehend:listTargetedSentimentDetectionJobs",
        "comprehend:listTopicsDetectionJobs",
        "compute-optimizer:getAutoScalingGroupRecommendations",
        "compute-optimizer:getEBSVolumeRecommendations",
        "compute-optimizer:getEC2InstanceRecommendations",
        "compute-optimizer:getEC2RecommendationProjectedMetrics",
        "compute-optimizer:getECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:getECSServiceRecommendations",
        "compute-optimizer:getEnrollmentStatus",
        "compute-optimizer:getIdleRecommendations",
        "compute-optimizer:getRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:getRDSDatabaseRecommendations",
        "compute-optimizer:getRecommendationSummaries",
        "config:batchGetAggregateResourceConfig",
        "config:batchGetResourceConfig",
        "config:describeAggregateComplianceByConfigRules",
        "config:describeAggregationAuthorizations",
        "config:describeComplianceByConfigRule",
        "config:describeComplianceByResource",
        "config:describeConfigRuleEvaluationStatus",
        "config:describeConfigRules",
        "config:describeConfigurationAggregators",
        "config:describeConfigurationAggregatorSourcesStatus",
        "config:describeConfigurationRecorders",
        "config:describeConfigurationRecorderStatus",
        "config:describeConformancePackCompliance",
        "config:describeConformancePacks",
        "config:describeConformancePackStatus",
        "config:describeDeliveryChannels",
        "config:describeDeliveryChannelStatus",
        "config:describeOrganizationConfigRules",
        "config:describeOrganizationConfigRuleStatuses",
        "config:describeOrganizationConformancePacks",
        "config:describeOrganizationConformancePackStatuses",
        "config:describePendingAggregationRequests",
        "config:describeRemediationConfigurations",
```

```
        "config:describeRemediationExceptions",
        "config:describeRemediationExecutionStatus",
        "config:describeRetentionConfigurations",
        "config:getAggregateComplianceDetailsByConfigRule",
        "config:getAggregateConfigRuleComplianceSummary",
        "config:getAggregateDiscoveredResourceCounts",
        "config:getAggregateResourceConfig",
        "config:getComplianceDetailsByConfigRule",
        "config:getComplianceDetailsByResource",
        "config:getComplianceSummaryByConfigRule",
        "config:getComplianceSummaryByResourceType",
        "config:getConformancePackComplianceDetails",
        "config:getConformancePackComplianceSummary",
        "config:getDiscoveredResourceCounts",
        "config:getOrganizationConfigRuleDetailedStatus",
        "config:getOrganizationConformancePackDetailedStatus",
        "config:getResourceConfigHistory",
        "config:listAggregateDiscoveredResources",
        "config:listDiscoveredResources",
        "config:listTagsForResource",
        "config:selectAggregateResourceConfig",
        "config:selectResourceConfig",
        "connect:batchGetFlowAssociation",
        "connect:describeContact",
        "connect:describeContactFlow",
        "connect:describeInstance",
        "connect:describeInstanceAttribute",
        "connect:describePhoneNumber",
        "connect:describeQueue",
        "connect:describeQuickConnect",
        "connect:describeRoutingProfile",
        "connect:describeUser",
        "connect:describeUserHierarchyStructure",
        "connect:getCurrentMetricData",
        "connect:getMetricData",
        "connect:getMetricDataV2",
        "connect:listContactEvaluations",
        "connect:listEvaluationForms",
        "connect:listEvaluationFormVersions",
        "connect:listInstanceAttributes",
        "connect:listInstanceStorageConfigs",
        "connect:listPhoneNumbersV2",
        "connect:listQueueQuickConnects",
        "connect:listQueues",
```

```
        "connect:listQuickConnects",
        "connect:listRoutingProfileQueues",
        "connect:listRoutingProfiles",
        "connect:listSecurityProfiles",
        "connect:listSecurityProfilePermissions",
        "connect:listUsers",
        "connect:listViews",
        "connect:listViewVersions",
        "connect:searchQueues",
        "connect:searchRoutingProfiles",
        "connect:searchUsers",
        "connect-campaigns:describeCampaign",
        "controlcatalog:getControl",
        "controltower:describeAccountFactoryConfig",
        "controltower:describeCoreService",
        "controltower:describeGuardrail",
        "controltower:describeGuardrailForTarget",
        "controltower:describeManagedAccount",
        "controltower:describeSingleSignOn",
        "controltower:getAvailableUpdates",
        "controltower:getBaselineOperation",
        "controltower:getControlOperation",
        "controltower:getEnabledBaseline",
        "controltower:getEnabledControl",
        "controltower:getHomeRegion",
        "controltower:getLandingZone",
        "controltower:getLandingZoneStatus",
        "controltower:listBaselines",
        "controltower:listDirectoryGroups",
        "controltower:listEnabledControls",
        "controltower:listEnabledBaselines",
        "controltower:listGuardrailsForTarget",
        "controltower:listGuardrailViolations",
        "controltower:listLandingZones",
        "controltower:listManagedAccounts",
        "controltower:listManagedAccountsForGuardrail",
        "controltower:listManagedAccountsForParent",
        "controltower:listManagedOrganizationalUnits",
        "controltower:listManagedOrganizationalUnitsForGuardrail",
        "cost-optimization-hub:getPreferences",
        "cost-optimization-hub:getRecommendation",
        "cost-optimization-hub:listEnrollmentStatuses",
        "cost-optimization-hub:listRecommendations",
        "cost-optimization-hub:listRecommendationSummaries",
```

```
        "databrew:describeDataset",
        "databrew:describeJob",
        "databrew:describeProject",
        "databrew:describeRecipe",
        "databrew:listDatasets",
        "databrew:listJobRuns",
        "databrew:listJobs",
        "databrew:listProjects",
        "databrew:listRecipes",
        "databrew:listRecipeVersions",
        "databrew:listTagsForResource",
        "datapipeline:describeObjects",
        "datapipeline:describePipelines",
        "datapipeline:getPipelineDefinition",
        "datapipeline:listPipelines",
        "datapipeline:queryObjects",
        "datasync:describeAgent",
        "datasync:describeLocationAzureBlob",
        "datasync:describeLocationEfs",
        "datasync:describeLocationFsxLustre",
        "datasync:describeLocationFsxOntap",
        "datasync:describeLocationFsxOpenZfs",
        "datasync:describeLocationFsxWindows",
        "datasync:describeLocationHdfs",
        "datasync:describeLocationNfs",
        "datasync:describeLocationObjectStorage",
        "datasync:describeLocationS3",
        "datasync:describeLocationSmb",
        "datasync:describeTask",
        "datasync:describeTaskExecution",
        "datasync:listAgents",
        "datasync:listLocations",
        "datasync:listTaskExecutions",
        "datasync:listTasks",
        "datazone:getAsset",
        "datazone:getAssetType",
        "datazone:getDataSource",
        "datazone:getDataSourceRun",
        "datazone:getDomain",
        "datazone:getEnvironment",
        "datazone:getEnvironmentBlueprint",
        "datazone:getEnvironmentBlueprintConfiguration",
        "datazone:getEnvironmentProfile",
        "datazone:getFormType",
```

```
        "datazone:getGlossary",
        "datazone:getGlossaryTerm",
        "datazone:getGroupProfile",
        "datazone:getListing",
        "datazone:getMetadataGenerationRun",
        "datazone:getProject",
        "datazone:getSubscription",
        "datazone:getSubscriptionGrant",
        "datazone:getSubscriptionRequestDetails",
        "datazone:getSubscriptionTarget",
        "datazone:getUserProfile",
        "datazone:listAssetRevisions",
        "datazone:listDataSourceRunActivities",
        "datazone:listDataSourceRuns",
        "datazone:listDataSources",
        "datazone:listDomains",
        "datazone:listEnvironmentBlueprintConfigurations",
        "datazone:listEnvironmentBlueprints",
        "datazone:listEnvironmentProfiles",
        "datazone:listEnvironments",
        "datazone:listMetadataGenerationRuns",
        "datazone:listProjectMemberships",
        "datazone:listProjects",
        "datazone:listSubscriptionGrants",
        "datazone:listSubscriptionRequests",
        "datazone:listSubscriptions",
        "datazone:listSubscriptionTargets",
        "datazone:getAssetFilter",
        "datazone:getDomainUnit",
        "datazone:getLineageNode",
        "datazone:getProjectProfile",
        "datazone:getRule",
        "datazone:listAssetFilters",
        "datazone:listConnections",
        "datazone:listDomainUnitsForParent",
        "datazone:listEntityOwners",
        "datazone:listLineageNodeHistory",
        "datazone:listNotifications",
        "datazone:listPolicyGrants",
        "datazone:listProjectProfiles",
        "datazone:listRules",
        "datazone:searchGroupProfiles",
        "datazone:searchUserProfiles",
        "dax:describeClusters",
```

```
        "dax:describeDefaultParameters",
        "dax:describeEvents",
        "dax:describeParameterGroups",
        "dax:describeParameters",
        "dax:describeSubnetGroups",
        "deadline:listAvailableMeteredProducts",
        "deadline:listBudgets",
        "deadline:listFarmMembers",
        "deadline:listFarms",
        "deadline:listFleetMembers",
        "deadline:listFleets",
        "deadline:listJobMembers",
        "deadline:listJobs",
        "deadline:listLicenseEndpoints",
        "deadline:listMeteredProducts",
        "deadline:listMonitors",
        "deadline:listQueueEnvironments",
        "deadline:listQueueFleetAssociations",
        "deadline:listQueueMembers",
        "deadline:listQueues",
        "deadline:listStorageProfiles",
        "deadline:listWorkers",
        "detective:getMembers",
        "detective:listGraphs",
        "detective:listInvitations",
        "detective:listMembers",
        "devicefarm:getAccountSettings",
        "devicefarm:getDevice",
        "devicefarm:getDevicePool",
        "devicefarm:getDevicePoolCompatibility",
        "devicefarm:getJob",
        "devicefarm:getOfferingStatus",
        "devicefarm:getProject",
        "devicefarm:getRemoteAccessSession",
        "devicefarm:getRun",
        "devicefarm:getSuite",
        "devicefarm:getTest",
        "devicefarm:getTestGridProject",
        "devicefarm:getTestGridSession",
        "devicefarm:getUpload",
        "devicefarm:getVPCEConfiguration",
        "devicefarm:listArtifacts",
        "devicefarm:listDevicePools",
        "devicefarm:listDevices",
```

```
        "devicefarm:listJobs",
        "devicefarm:listNetworkProfiles",
        "devicefarm:listOfferingPromotions",
        "devicefarm:listOfferingTransactions",
        "devicefarm:listProjects",
        "devicefarm:listRemoteAccessSessions",
        "devicefarm:listRuns",
        "devicefarm:listSamples",
        "devicefarm:listSuites",
        "devicefarm:listTestGridProjects",
        "devicefarm:listTestGridSessionActions",
        "devicefarm:listTestGridSessionArtifacts",
        "devicefarm:listTestGridSessions",
        "devicefarm:listTests",
        "devicefarm:listUniqueProblems",
        "devicefarm:listUploads",
        "devicefarm:listVPCEConfigurations",
        "directconnect:describeConnectionLoa",
        "directconnect:describeConnections",
        "directconnect:describeConnectionsOnInterconnect",
        "directconnect:describeCustomerMetadata",
        "directconnect:describeDirectConnectGatewayAssociationProposals",
        "directconnect:describeDirectConnectGatewayAssociations",
        "directconnect:describeDirectConnectGatewayAttachments",
        "directconnect:describeDirectConnectGateways",
        "directconnect:describeHostedConnections",
        "directconnect:describeInterconnectLoa",
        "directconnect:describeInterconnects",
        "directconnect:describeLags",
        "directconnect:describeLoa",
        "directconnect:describeLocations",
        "directconnect:describeRouterConfiguration",
        "directconnect:describeVirtualGateways",
        "directconnect:describeVirtualInterfaces",
        "directconnect:listVirtualInterfaceTestHistory",
        "dlm:getLifecyclePolicies",
        "dlm:getLifecyclePolicy",
        "dms:describeAccountAttributes",
        "dms:describeApplicableIndividualAssessments",
        "dms:describeCertificates",
        "dms:describeConnections",
        "dms:describeEndpoints",
        "dms:describeEndpointSettings",
        "dms:describeEndpointTypes",
```

```
            "dms:describeEventCategories",
            "dms:describeEvents",
            "dms:describeEventSubscriptions",
            "dms:describeFleetAdvisorCollectors",
            "dms:describeFleetAdvisorDatabases",
            "dms:describeFleetAdvisorLsaAnalysis",
            "dms:describeFleetAdvisorSchemaObjectSummary",
            "dms:describeFleetAdvisorSchemas",
            "dms:describeOrderableReplicationInstances",
            "dms:describePendingMaintenanceActions",
            "dms:describeRefreshSchemasStatus",
            "dms:describeReplicationConfigs",
            "dms:describeReplicationInstances",
            "dms:describeReplicationInstanceTaskLogs",
            "dms:describeReplications",
            "dms:describeReplicationSubnetGroups",
            "dms:describeReplicationTableStatistics",
            "dms:describeReplicationTaskAssessmentResults",
            "dms:describeReplicationTaskAssessmentRuns",
            "dms:describeReplicationTaskIndividualAssessments",
            "dms:describeReplicationTasks",
            "dms:describeSchemas",
            "dms:describeTableStatistics",
            "docdb-elastic:getCluster",
            "docdb-elastic:getClusterSnapshot",
            "docdb-elastic:listClusters",
            "docdb-elastic:listClusterSnapshots",
            "drs:describeJobLogItems",
            "drs:describeJobs",
            "drs:describeLaunchConfigurationTemplates",
            "drs:describeRecoveryInstances",
            "drs:describeRecoverySnapshots",
            "drs:describeReplicationConfigurationTemplates",
            "drs:describeSourceNetworks",
            "drs:describeSourceServers",
            "drs:getLaunchConfiguration",
            "drs:getReplicationConfiguration",
            "drs:listExtensibleSourceServers",
            "drs:listLaunchActions",
            "drs:listStagingAccounts",
            "ds:describeClientAuthenticationSettings",
            "ds:describeConditionalForwarders",
            "ds:describeDirectories",
            "ds:describeDomainControllers",
```

```
        "ds:describeEventTopics",
        "ds:describeHybridADUpdate",
        "ds:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
        "ds:getSnapshotLimits",
        "ds:listIpRoutes",
        "ds:listSchemaExtensions",
        "ds:listTagsForResource",
        "dsql:getCluster",
        "dsql:getVpcEndpointServiceName",
        "dsql:listClusters",
        "dynamodb:describeBackup",
        "dynamodb:describeContinuousBackups",
        "dynamodb:describeContributorInsights",
        "dynamodb:describeExport",
        "dynamodb:describeGlobalTable",
        "dynamodb:describeGlobalTableSettings",
        "dynamodb:describeImport",
        "dynamodb:describeKinesisStreamingDestination",
        "dynamodb:describeLimits",
        "dynamodb:describeStream",
        "dynamodb:describeTable",
        "dynamodb:describeTableReplicaAutoScaling",
        "dynamodb:describeTimeToLive",
        "dynamodb:getResourcePolicy",
        "dynamodb:listBackups",
        "dynamodb:listContributorInsights",
        "dynamodb:listExports",
        "dynamodb:listGlobalTables",
        "dynamodb:listImports",
        "dynamodb:listStreams",
        "dynamodb:listTables",
        "dynamodb:listTagsOfResource",
        "ebs:listChangedBlocks",
        "ebs:listSnapshotBlocks",
        "ec2:describeAccountAttributes",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
        "ec2:describeAddressTransfers",
        "ec2:describeAggregateIdFormat",
        "ec2:describeAvailabilityZones",
```

```
        "ec2:describeBundleTasks",
        "ec2:describeByoipCidrs",
        "ec2:describeCapacityBlockOfferings",
        "ec2:describeCapacityBlocks",
        "ec2:describeCapacityBlockStatus",
        "ec2:describeCapacityManagerDataExports",
        "ec2:describeCapacityReservationFleets",
        "ec2:describeCapacityReservations",
        "ec2:describeCapacityReservationTopology",
        "ec2:describeCarrierGateways",
        "ec2:describeClassicLinkInstances",
        "ec2:describeClientVpnAuthorizationRules",
        "ec2:describeClientVpnConnections",
        "ec2:describeClientVpnEndpoints",
        "ec2:describeClientVpnRoutes",
        "ec2:describeClientVpnTargetNetworks",
        "ec2:describeCoipPools",
        "ec2:describeConversionTasks",
        "ec2:describeCustomerGateways",
        "ec2:describeDhcpOptions",
        "ec2:describeEgressOnlyInternetGateways",
        "ec2:describeExportImageTasks",
        "ec2:describeExportTasks",
        "ec2:describeFastLaunchImages",
        "ec2:describeFastSnapshotRestores",
        "ec2:describeFleetHistory",
        "ec2:describeFleetInstances",
        "ec2:describeFleets",
        "ec2:describeFlowLogs",
        "ec2:describeFpgaImageAttribute",
        "ec2:describeFpgaImages",
        "ec2:describeHostReservationOfferings",
        "ec2:describeHostReservations",
        "ec2:describeHosts",
        "ec2:describeIamInstanceProfileAssociations",
        "ec2:describeIdentityIdFormat",
        "ec2:describeIdFormat",
        "ec2:describeImageAttribute",
        "ec2:describeImages",
        "ec2:describeImportImageTasks",
        "ec2:describeImportSnapshotTasks",
        "ec2:describeInstanceAttribute",
        "ec2:describeInstanceConnectEndpoints",
        "ec2:describeInstanceCreditSpecifications",
```

```
        "ec2:describeInstanceEventNotificationAttributes",
        "ec2:describeInstanceEventWindows",
        "ec2:describeInstances",
        "ec2:describeInstanceStatus",
        "ec2:describeInstanceTypeOfferings",
        "ec2:describeInstanceTypes",
        "ec2:describeInstanceTopology",
        "ec2:describeInternetGateways",
        "ec2:describeIpamByoasn",
        "ec2:describeIpamExternalResourceVerificationTokens",
        "ec2:describeIpamPools",
        "ec2:describeIpamResourceDiscoveries",
        "ec2:describeIpamResourceDiscoveryAssociations",
        "ec2:describeIpams",
        "ec2:describeIpamScopes",
        "ec2:describeIpv6Pools",
        "ec2:describeKeyPairs",
        "ec2:describeLaunchTemplates",
        "ec2:describeLaunchTemplateVersions",
        "ec2:describeLocalGatewayRouteTables",
        "ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:describeLocalGatewayRouteTableVpcAssociations",
        "ec2:describeLocalGateways",
        "ec2:describeLocalGatewayVirtualInterfaceGroups",
        "ec2:describeLocalGatewayVirtualInterfaces",
        "ec2:describeManagedPrefixLists",
        "ec2:describeMovingAddresses",
        "ec2:describeNatGateways",
        "ec2:describeNetworkAcls",
        "ec2:describeNetworkInsightsAccessScopeAnalyses",
        "ec2:describeNetworkInsightsAccessScopes",
        "ec2:describeNetworkInsightsAnalyses",
        "ec2:describeNetworkInsightsPaths",
        "ec2:describeNetworkInterfaceAttribute",
        "ec2:describeNetworkInterfaces",
        "ec2:describeOutpostLags",
        "ec2:describePlacementGroups",
        "ec2:describePrefixLists",
        "ec2:describePrincipalIdFormat",
        "ec2:describePublicIpv4Pools",
        "ec2:describeRegions",
        "ec2:describeReplaceRootVolumeTasks",
        "ec2:describeReservedInstances",
        "ec2:describeReservedInstancesListings",
```

```
        "ec2:describeReservedInstancesModifications",
        "ec2:describeReservedInstancesOfferings",
        "ec2:describeRouteServerEndpoints",
        "ec2:describeRouteServerPeers",
        "ec2:describeRouteServers",
        "ec2:describeRouteTables",
        "ec2:describeScheduledInstanceAvailability",
        "ec2:describeScheduledInstances",
        "ec2:describeSecurityGroupReferences",
        "ec2:describeSecurityGroupRules",
        "ec2:describeSecurityGroups",
        "ec2:describeServiceLinkVirtualInterfaces",
        "ec2:describeSnapshotAttribute",
        "ec2:describeSnapshots",
        "ec2:describeSnapshotTierStatus",
        "ec2:describeSpotDatafeedSubscription",
        "ec2:describeSpotFleetInstances",
        "ec2:describeSpotFleetRequestHistory",
        "ec2:describeSpotFleetRequests",
        "ec2:describeSpotInstanceRequests",
        "ec2:describeSpotPriceHistory",
        "ec2:describeStaleSecurityGroups",
        "ec2:describeStoreImageTasks",
        "ec2:describeSubnets",
        "ec2:describeTags",
        "ec2:describeTrafficMirrorFilterRules",
        "ec2:describeTrafficMirrorFilters",
        "ec2:describeTrafficMirrorSessions",
        "ec2:describeTrafficMirrorTargets",
        "ec2:describeTransitGatewayAttachments",
        "ec2:describeTransitGatewayConnectPeers",
        "ec2:describeTransitGatewayConnects",
        "ec2:describeTransitGatewayMeteringPolicies",
        "ec2:describeTransitGatewayMulticastDomains",
        "ec2:describeTransitGatewayPeeringAttachments",
        "ec2:describeTransitGatewayPolicyTables",
        "ec2:describeTransitGatewayRouteTableAnnouncements",
        "ec2:describeTransitGatewayRouteTables",
        "ec2:describeTransitGateways",
        "ec2:describeTransitGatewayVpcAttachments",
        "ec2:describeVerifiedAccessEndpoints",
        "ec2:describeVerifiedAccessGroups",
        "ec2:describeVerifiedAccessInstanceLoggingConfigurations",
        "ec2:describeVerifiedAccessInstances",
```

```
        "ec2:describeVerifiedAccessInstanceWebAclAssociations",
        "ec2:describeVerifiedAccessTrustProviders",
        "ec2:describeVolumeAttribute",
        "ec2:describeVolumes",
        "ec2:describeVolumesModifications",
        "ec2:describeVolumeStatus",
        "ec2:describeVpcAttribute",
        "ec2:describeVpcBlockPublicAccessExclusions",
        "ec2:describeVpcBlockPublicAccessOptions",
        "ec2:describeVpcClassicLink",
        "ec2:describeVpcClassicLinkDnsSupport",
        "ec2:describeVpcEndpointAssociations",
        "ec2:describeVpcEndpointConnectionNotifications",
        "ec2:describeVpcEndpointConnections",
        "ec2:describeVpcEndpoints",
        "ec2:describeVpcEndpointServiceConfigurations",
        "ec2:describeVpcEndpointServicePermissions",
        "ec2:describeVpcEndpointServices",
        "ec2:describeVpcEncryptionControls",
        "ec2:describeVpcPeeringConnections",
        "ec2:describeVpcs",
        "ec2:describeVpnConnections",
        "ec2:describeVpnGateways",
        "ec2:getAssociatedEnclaveCertificateIamRoles",
        "ec2:getAssociatedIpv6PoolCidrs",
        "ec2:getCapacityManagerAttributes",
        "ec2:getCapacityManagerMetricData",
        "ec2:getCapacityManagerMetricDimensions",
        "ec2:getCapacityReservationUsage",
        "ec2:getCoipPoolUsage",
        "ec2:getConsoleOutput",
        "ec2:getConsoleScreenshot",
        "ec2:getDefaultCreditSpecification",
        "ec2:getEbsDefaultKmsKeyId",
        "ec2:getEbsEncryptionByDefault",
        "ec2:getGroupsForCapacityReservation",
        "ec2:getHostReservationPurchasePreview",
        "ec2:getImageBlockPublicAccessState",
        "ec2:getInstanceTypesFromInstanceRequirements",
        "ec2:getIpamAddressHistory",
        "ec2:getIpamDiscoveredAccounts",
        "ec2:getIpamDiscoveredPublicAddresses",
        "ec2:getIpamDiscoveredResourceCidrs",
        "ec2:getIpamPoolAllocations",
```

```
        "ec2:getIpamPoolCidrs",
        "ec2:getIpamResourceCidrs",
        "ec2:getLaunchTemplateData",
        "ec2:getManagedPrefixListAssociations",
        "ec2:getManagedPrefixListEntries",
        "ec2:getNetworkInsightsAccessScopeContent",
        "ec2:getReservedInstancesExchangeQuote",
        "ec2:getRouteServerAssociations",
        "ec2:getRouteServerPropagations",
        "ec2:getRouteServerRoutingDatabase",
        "ec2:getSerialConsoleAccessStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:getSpotPlacementScores",
        "ec2:getSubnetCidrReservations",
        "ec2:getTransitGatewayAttachmentPropagations",
        "ec2:getTransitGatewayMulticastDomainAssociations",
        "ec2:getTransitGatewayPolicyTableAssociations",
        "ec2:getTransitGatewayPolicyTableEntries",
        "ec2:getTransitGatewayPrefixListReferences",
        "ec2:getTransitGatewayRouteTableAssociations",
        "ec2:getTransitGatewayRouteTablePropagations",
        "ec2:getVerifiedAccessEndpointPolicy",
        "ec2:getVerifiedAccessGroupPolicy",
        "ec2:getVpcResourcesBlockingEncryptionEnforcement",
        "ec2:getVpnTunnelReplacementStatus",
        "ec2:listImagesInRecycleBin",
        "ec2:listSnapshotsInRecycleBin",
        "ec2:searchLocalGatewayRoutes",
        "ec2:searchTransitGatewayMulticastGroups",
        "ec2:searchTransitGatewayRoutes",
        "ecr-public:describeImages",
        "ecr-public:describeImageTags",
        "ecr-public:describeRegistries",
        "ecr-public:describeRepositories",
        "ecr-public:getRegistryCatalogData",
        "ecr-public:getRepositoryCatalogData",
```

```
        "ecr-public:getRepositoryPolicy",
        "ecr-public:listTagsForResource",
        "ecr:batchCheckLayerAvailability",
        "ecr:batchGetImage",
        "ecr:batchGetRepositoryScanningConfiguration",
        "ecr:describeImageReplicationStatus",
        "ecr:describeImages",
        "ecr:describeImageScanFindings",
        "ecr:describeImageSigningStatus",
        "ecr:describePullThroughCacheRules",
        "ecr:describeRegistry",
        "ecr:describeRepositories",
        "ecr:describeRepositoryCreationTemplates",
        "ecr:getAccountSetting",
        "ecr:getAuthorizationToken",
        "ecr:getDownloadUrlForLayer",
        "ecr:getLifecyclePolicy",
        "ecr:getLifecyclePolicyPreview",
        "ecr:getRegistryPolicy",
        "ecr:getRegistryScanningConfiguration",
        "ecr:getRepositoryPolicy",
        "ecr:getSigningConfiguration",
        "ecr:listImages",
        "ecr:listPullTimeUpdateExclusions",
        "ecr:listTagsForResource",
        "ecs:describeCapacityProviders",
        "ecs:describeClusters",
        "ecs:describeContainerInstances",
        "ecs:describeExpressGatewayService",
        "ecs:describeServiceDeployments",
        "ecs:describeServiceRevisions",
        "ecs:describeServices",
        "ecs:describeTaskDefinition",
        "ecs:describeTasks",
        "ecs:describeTaskSets",
        "ecs:getTaskProtection",
        "ecs:listAccountSettings",
        "ecs:listAttributes",
        "ecs:listClusters",
        "ecs:listContainerInstances",
        "ecs:listServiceDeployments",
        "ecs:listServices",
        "ecs:listServicesByNamespace",
        "ecs:listTagsForResource",
```

```
        "ecs:listTaskDefinitionFamilies",
        "ecs:listTaskDefinitions",
        "ecs:listTasks",
        "eks:describeAccessEntry",
        "eks:describeAddon",
        "eks:describeAddonConfiguration",
        "eks:describeAddonVersions",
        "eks:describeCapability",
        "eks:describeCluster",
        "eks:describeClusterVersions",
        "eks:describeEksAnywhereSubscription",
        "eks:describeFargateProfile",
        "eks:describeIdentityProviderConfig",
        "eks:describeInsight",
        "eks:describeNodegroup",
        "eks:describePodIdentityAssociation",
        "eks:describeUpdate",
        "eks:listAccessEntries",
        "eks:listAccessPolicies",
        "eks:listAddons",
        "eks:listAssociatedAccessPolicies",
        "eks:listCapabilities",
        "eks:listClusters",
        "eks:listEksAnywhereSubscriptions",
        "eks:listFargateProfiles",
        "eks:listIdentityProviderConfigs",
        "eks:listInsights",
        "eks:listNodegroups",
        "eks:listPodIdentityAssociations",
        "eks:listUpdates",
        "elasticache:describeCacheClusters",
        "elasticache:describeCacheEngineVersions",
        "elasticache:describeCacheParameterGroups",
        "elasticache:describeCacheParameters",
        "elasticache:describeCacheSecurityGroups",
        "elasticache:describeCacheSubnetGroups",
        "elasticache:describeEngineDefaultParameters",
        "elasticache:describeEvents",
        "elasticache:describeGlobalReplicationGroups",
        "elasticache:describeReplicationGroups",
        "elasticache:describeReservedCacheNodes",
        "elasticache:describeReservedCacheNodesOfferings",
        "elasticache:describeServerlessCaches",
        "elasticache:describeServerlessCacheSnapshots",
```

```
        "elasticache:describeServiceUpdates",
        "elasticache:describeSnapshots",
        "elasticache:describeUpdateActions",
        "elasticache:describeUserGroups",
        "elasticache:describeUsers",
        "elasticache:listAllowedNodeTypeModifications",
        "elasticache:listTagsForResource",
        "elasticbeanstalk:checkDNSAvailability",
        "elasticbeanstalk:describeAccountAttributes",
        "elasticbeanstalk:describeApplications",
        "elasticbeanstalk:describeApplicationVersions",
        "elasticbeanstalk:describeConfigurationOptions",
        "elasticbeanstalk:describeEnvironmentHealth",
        "elasticbeanstalk:describeEnvironmentManagedActionHistory",
        "elasticbeanstalk:describeEnvironmentManagedActions",
        "elasticbeanstalk:describeEnvironmentResources",
        "elasticbeanstalk:describeEnvironments",
        "elasticbeanstalk:describeEvents",
        "elasticbeanstalk:describeInstancesHealth",
        "elasticbeanstalk:describePlatformVersion",
        "elasticbeanstalk:listAvailableSolutionStacks",
        "elasticbeanstalk:listPlatformBranches",
        "elasticbeanstalk:listPlatformVersions",
        "elasticbeanstalk:listTagsForResource",
        "elasticbeanstalk:describeConfigurationSettings",
        "elasticbeanstalk:validateConfigurationSettings",
        "elasticfilesystem:describeAccessPoints",
        "elasticfilesystem:describeBackupPolicy",
        "elasticfilesystem:describeFileSystemPolicy",
        "elasticfilesystem:describeFileSystems",
        "elasticfilesystem:describeLifecycleConfiguration",
        "elasticfilesystem:describeMountTargets",
        "elasticfilesystem:describeMountTargetSecurityGroups",
        "elasticfilesystem:describeReplicationConfigurations",
        "elasticfilesystem:describeTags",
        "elasticfilesystem:listTagsForResource",
        "elasticloadbalancing:describeAccountLimits",
        "elasticloadbalancing:describeInstanceHealth",
        "elasticloadbalancing:describeListenerCertificates",
        "elasticloadbalancing:describeListeners",
        "elasticloadbalancing:describeLoadBalancerAttributes",
        "elasticloadbalancing:describeLoadBalancerPolicies",
        "elasticloadbalancing:describeLoadBalancerPolicyTypes",
        "elasticloadbalancing:describeLoadBalancers",
```

```
        "elasticloadbalancing:describeRules",
        "elasticloadbalancing:describeSSLPolicies",
        "elasticloadbalancing:describeTags",
        "elasticloadbalancing:describeTargetGroupAttributes",
        "elasticloadbalancing:describeTargetGroups",
        "elasticloadbalancing:describeTargetHealth",
        "elasticloadbalancing:describeTrustStoreAssociations",
        "elasticloadbalancing:describeTrustStoreRevocations",
        "elasticloadbalancing:describeTrustStores",
        "elasticmapreduce:describeCluster",
        "elasticmapreduce:describeNotebookExecution",
        "elasticmapreduce:describePersistentAppUI",
        "elasticmapreduce:describeReleaseLabel",
        "elasticmapreduce:describeSecurityConfiguration",
        "elasticmapreduce:describeStep",
        "elasticmapreduce:describeStudio",
        "elasticmapreduce:getAutoTerminationPolicy",
        "elasticmapreduce:getBlockPublicAccessConfiguration",
        "elasticmapreduce:getManagedScalingPolicy",
        "elasticmapreduce:getStudioSessionMapping",
        "elasticmapreduce:listBootstrapActions",
        "elasticmapreduce:listClusters",
        "elasticmapreduce:listInstanceFleets",
        "elasticmapreduce:listInstanceGroups",
        "elasticmapreduce:listInstances",
        "elasticmapreduce:listNotebookExecutions",
        "elasticmapreduce:listReleaseLabels",
        "elasticmapreduce:listSecurityConfigurations",
        "elasticmapreduce:listSteps",
        "elasticmapreduce:listStudios",
        "elasticmapreduce:listStudioSessionMappings",
        "elasticmapreduce:listSupportedInstanceTypes",
        "emr-containers:describeJobRun",
        "emr-containers:describeJobTemplate",
        "emr-containers:describeManagedEndpoint",
        "emr-containers:describeVirtualCluster",
        "emr-containers:listJobRuns",
        "emr-containers:listJobTemplates",
        "emr-containers:listManagedEndpoints",
        "emr-containers:listVirtualClusters",
        "emr-serverless:getApplication",
        "emr-serverless:getJobRun",
        "emr-serverless:listApplications",
        "emr-serverless:listJobRunAttempts",
```

```
        "emr-serverless:listJobRuns",
        "entityresolution:getIdMappingJob",
        "entityresolution:getIdMappingWorkflow",
        "entityresolution:getMatchingJob",
        "entityresolution:getMatchingWorkflow",
        "entityresolution:getProviderService",
        "entityresolution:getSchemaMapping",
        "entityresolution:listIdMappingJobs",
        "entityresolution:listIdMappingWorkflows",
        "entityresolution:listMatchingJobs",
        "entityresolution:listMatchingWorkflows",
        "entityresolution:listProviderServices",
        "entityresolution:listSchemaMappings",
        "es:describeDomain",
        "es:describeDomainAutoTunes",
        "es:describeDomainChangeProgress",
        "es:describeDomainConfig",
        "es:describeDomainHealth",
        "es:describeDomainNodes",
        "es:describeDomains",
        "es:describeDryRunProgress",
        "es:describeElasticsearchDomain",
        "es:describeElasticsearchDomainConfig",
        "es:describeElasticsearchDomains",
        "es:getApplication",
        "es:getCapability",
        "es:getDataSource",
        "es:getDefaultApplicationSetting",
        "es:getDirectQueryDataSource",
        "es:getDomainMaintenanceStatus",
        "es:describeInboundConnections",
        "es:describeInstanceTypeLimits",
        "es:describeInsightDetails",
        "es:describeOutboundConnections",
        "es:describePackages",
        "es:describeReservedInstanceOfferings",
        "es:describeReservedInstances",
        "es:describeVpcEndpoints",
        "es:getCompatibleVersions",
        "es:getPackageVersionHistory",
        "es:getUpgradeHistory",
        "es:getUpgradeStatus",
        "es:listApplications",
        "es:listDataSources",
```

```
        "es:listDirectQueryDataSources",
        "es:listDomainMaintenances",
        "es:listDomainNames",
        "es:listDomainsForPackage",
        "es:listInstanceTypeDetails",
        "es:listInsights",
        "es:listPackagesForDomain",
        "es:listScheduledActions",
        "es:listTags",
        "es:listVersions",
        "es:listVpcEndpointAccess",
        "es:listVpcEndpoints",
        "es:listVpcEndpointsForDomain",
        "events:describeApiDestination",
        "events:describeArchive",
        "events:describeConnection",
        "events:describeEndpoint",
        "events:describeEventBus",
        "events:describeEventSource",
        "events:describePartnerEventSource",
        "events:describeReplay",
        "events:describeRule",
        "events:listApiDestinations",
        "events:listArchives",
        "events:listConnections",
        "events:listEndpoints",
        "events:listEventBuses",
        "events:listEventSources",
        "events:listPartnerEventSourceAccounts",
        "events:listPartnerEventSources",
        "events:listReplays",
        "events:listRuleNamesByTarget",
        "events:listRules",
        "events:listTargetsByRule",
        "events:testEventPattern",
        "evs:getEnvironment",
        "evs:getVersions",
        "evs:listEnvironmentHosts",
        "evs:listEnvironments",
        "evs:listEnvironmentVlans",
        "evs:listTagsForResource",
        "firehose:describeDeliveryStream",
        "firehose:listDeliveryStreams",
        "fis:getAction",
```

```
        "fis:getExperiment",
        "fis:getExperimentTargetAccountConfiguration",
        "fis:getExperimentTemplate",
        "fis:getSafetyLever",
        "fis:getTargetAccountConfiguration",
        "fis:listActions",
        "fis:listExperimentResolvedTargets",
        "fis:listExperimentTargetAccountConfigurations",
        "fis:listExperiments",
        "fis:listExperimentTemplates",
        "fis:listTargetAccountConfigurations",
        "fms:getAdminAccount",
        "fms:getAdminScope",
        "fms:getAppsList",
        "fms:getComplianceDetail",
        "fms:getNotificationChannel",
        "fms:getProtocolsList",
        "fms:getPolicy",
        "fms:getProtectionStatus",
        "fms:getResourceSet",
        "fms:getThirdPartyFirewallAssociationStatus",
        "fms:getViolationDetails",
        "fms:listAdminAccountsForOrganization",
        "fms:listAdminsManagingAccount",
        "fms:listAppsLists",
        "fms:listComplianceStatus",
        "fms:listDiscoveredResources",
        "fms:listMemberAccounts",
        "fms:listProtocolsLists",
        "fms:listPolicies",
        "fms:listResourceSetResources",
        "fms:listResourceSets",
        "fms:listThirdPartyFirewallFirewallPolicies",
        "forecast:describeDataset",
        "forecast:describeDatasetGroup",
        "forecast:describeDatasetImportJob",
        "forecast:describeForecast",
        "forecast:describeForecastExportJob",
        "forecast:describePredictor",
        "forecast:getAccuracyMetrics",
        "forecast:listDatasetGroups",
        "forecast:listDatasetImportJobs",
        "forecast:listDatasets",
        "forecast:listForecastExportJobs",
```

```
        "forecast:listForecasts",
        "forecast:listPredictors",
        "freetier:getFreeTierUsage",
        "fsx:describeBackups",
        "fsx:describeDataRepositoryAssociations",
        "fsx:describeDataRepositoryTasks",
        "fsx:describeFileCaches",
        "fsx:describeFileSystems",
        "fsx:describeS3AccessPointAttachments",
        "fsx:describeSnapshots",
        "fsx:describeStorageVirtualMachines",
        "fsx:describeVolumes",
        "fsx:listTagsForResource",
        "gamelift:describeAlias",
        "gamelift:describeBuild",
        "gamelift:describeEC2InstanceLimits",
        "gamelift:describeFleetAttributes",
        "gamelift:describeFleetCapacity",
        "gamelift:describeFleetEvents",
        "gamelift:describeFleetLocationAttributes",
        "gamelift:describeFleetLocationCapacity",
        "gamelift:describeFleetLocationUtilization",
        "gamelift:describeFleetPortSettings",
        "gamelift:describeFleetUtilization",
        "gamelift:describeGameServer",
        "gamelift:describeGameServerGroup",
        "gamelift:describeGameSessionDetails",
        "gamelift:describeGameSessionPlacement",
        "gamelift:describeGameSessionQueues",
        "gamelift:describeGameSessions",
        "gamelift:describeInstances",
        "gamelift:describeMatchmaking",
        "gamelift:describeMatchmakingConfigurations",
        "gamelift:describeMatchmakingRuleSets",
        "gamelift:describePlayerSessions",
        "gamelift:describeRuntimeConfiguration",
        "gamelift:describeScalingPolicies",
        "gamelift:describeScript",
        "gamelift:listAliases",
        "gamelift:listBuilds",
        "gamelift:listFleets",
        "gamelift:listGameServerGroups",
        "gamelift:listGameServers",
        "gamelift:listScripts",
```

```
        "gamelift:resolveAlias",
        "geo:calculateRoute",
        "geo:calculateRouteMatrix",
        "geo:describeMap",
        "geo:describePlaceIndex",
        "geo:describeRouteCalculator",
        "geo:describeTracker",
        "geo:getMapGlyphs",
        "geo:getMapSprites",
        "geo:getMapStyleDescriptor",
        "geo:getMapTile",
        "geo:getPlace",
        "geo:listGeofenceCollections",
        "geo:listMaps",
        "geo:listPlaceIndexes",
        "geo:listRouteCalculators",
        "geo:listTrackerConsumers",
        "geo:searchPlaceIndexForPosition",
        "geo:searchPlaceIndexForSuggestions",
        "geo:searchPlaceIndexForText",
        "geo-maps:getStaticMap",
        "geo-maps:getTile",
        "geo-places:autocomplete",
        "geo-places:geocode",
        "geo-places:getPlace",
        "geo-places:reverseGeocode",
        "geo-places:searchNearby",
        "geo-places:searchText",
        "geo-places:suggest",
        "geo-routes:calculateIsolines",
        "geo-routes:calculateRouteMatrix",
        "geo-routes:calculateRoutes",
        "geo-routes:optimizeWaypoints",
        "geo-routes:snapToRoads",
        "glacier:describeJob",
        "glacier:describeVault",
        "glacier:getDataRetrievalPolicy",
        "glacier:getVaultAccessPolicy",
        "glacier:getVaultLock",
        "glacier:getVaultNotifications",
        "glacier:listJobs",
        "glacier:listTagsForVault",
        "glacier:listVaults",
        "globalaccelerator:describeAccelerator",
```

```
        "globalaccelerator:describeAcceleratorAttributes",
        "globalaccelerator:describeCrossAccountAttachment",
        "globalaccelerator:describeCustomRoutingAccelerator",
        "globalaccelerator:describeCustomRoutingAcceleratorAttributes",
        "globalaccelerator:describeCustomRoutingEndpointGroup",
        "globalaccelerator:describeCustomRoutingListener",
        "globalaccelerator:describeEndpointGroup",
        "globalaccelerator:describeListener",
        "globalaccelerator:listAccelerators",
        "globalaccelerator:listByoipCidrs",
        "globalaccelerator:listCrossAccountAttachments",
        "globalaccelerator:listCrossAccountResourceAccounts",
        "globalaccelerator:listCrossAccountResources",
        "globalaccelerator:listCustomRoutingAccelerators",
        "globalaccelerator:listCustomRoutingEndpointGroups",
        "globalaccelerator:listCustomRoutingListeners",
        "globalaccelerator:listCustomRoutingPortMappings",
        "globalaccelerator:listCustomRoutingPortMappingsByDestination",
        "globalaccelerator:listEndpointGroups",
        "globalaccelerator:listListeners",
        "glue:batchGetBlueprints",
        "glue:batchGetCrawlers",
        "glue:batchGetDevEndpoints",
        "glue:batchGetJobs",
        "glue:batchGetPartition",
        "glue:batchGetTriggers",
        "glue:batchGetWorkflows",
        "glue:checkSchemaVersionValidity",
        "glue:batchGetTableOptimizer",
        "glue:getBlueprint",
        "glue:getBlueprintRun",
        "glue:getBlueprintRuns",
        "glue:getCatalog",
        "glue:getCatalogImportStatus",
        "glue:getCatalogs",
        "glue:getClassifier",
        "glue:getClassifiers",
        "glue:getColumnStatisticsForPartition",
        "glue:getColumnStatisticsForTable",
        "glue:getColumnStatisticsTaskRun",
        "glue:getColumnStatisticsTaskRuns",
        "glue:getCompletion",
        "glue:getCrawler",
        "glue:getCrawlerMetrics",
```

```
        "glue:getCrawlers",
        "glue:getCustomEntityType",
        "glue:getDatabase",
        "glue:getDatabases",
        "glue:getDataCatalogEncryptionSettings",
        "glue:getDataflowGraph",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
        "glue:getDataQualityRuleset",
        "glue:getDataQualityRulesetEvaluationRun",
        "glue:getDevEndpoint",
        "glue:getDevEndpoints",
        "glue:getJob",
        "glue:getJobBookmark",
        "glue:getJobRun",
        "glue:getJobRuns",
        "glue:getJobs",
        "glue:getMapping",
        "glue:getMLTaskRun",
        "glue:getMLTaskRuns",
        "glue:getMLTransform",
        "glue:getMLTransforms",
        "glue:getPartition",
        "glue:getPartitionIndexes",
        "glue:getPartitions",
        "glue:getRegistry",
        "glue:getResourcePolicies",
        "glue:getResourcePolicy",
        "glue:getSchema",
        "glue:getSchemaByDefinition",
        "glue:getSchemaVersion",
        "glue:getSchemaVersionsDiff",
        "glue:getSecurityConfiguration",
        "glue:getSecurityConfigurations",
        "glue:getSession",
        "glue:getStatement",
        "glue:getTable",
        "glue:getTableOptimizer",
        "glue:getTableVersion",
        "glue:getTables",
        "glue:getTableVersions",
        "glue:getTrigger",
        "glue:getTriggers",
        "glue:getUserDefinedFunction",
```

```
        "glue:getUserDefinedFunctions",
        "glue:getWorkflow",
        "glue:getWorkflowRun",
        "glue:getWorkflowRuns",
        "glue:listColumnStatisticsTaskRuns",
        "glue:listCrawlers",
        "glue:listCrawls",
        "glue:listDataQualityResults",
        "glue:listDataQualityRuleRecommendationRuns",
        "glue:listDataQualityRulesetEvaluationRuns",
        "glue:listDataQualityRulesets",
        "glue:listDevEndpoints",
        "glue:listMLTransforms",
        "glue:listRegistries",
        "glue:listSchemas",
        "glue:listSchemaVersions",
        "glue:listSessions",
        "glue:listStatements",
        "glue:listTableOptimizerRuns",
        "glue:listTriggers",
        "glue:querySchemaVersionMetadata",
        "glue:startCompletion",
        "grafana:describeWorkspace",
        "grafana:describeWorkspaceAuthentication",
        "grafana:listPermissions",
        "grafana:listVersions",
        "grafana:listWorkspaces",
        "greengrass:describeComponent",
        "greengrass:getComponent",
        "greengrass:getConnectivityInfo",
        "greengrass:getCoreDefinition",
        "greengrass:getCoreDefinitionVersion",
        "greengrass:getCoreDevice",
        "greengrass:getDeployment",
        "greengrass:getDeploymentStatus",
        "greengrass:getDeviceDefinition",
        "greengrass:getDeviceDefinitionVersion",
        "greengrass:getFunctionDefinition",
        "greengrass:getFunctionDefinitionVersion",
        "greengrass:getGroup",
        "greengrass:getGroupCertificateAuthority",
        "greengrass:getGroupVersion",
        "greengrass:getLoggerDefinition",
        "greengrass:getLoggerDefinitionVersion",
```

```
        "greengrass:getResourceDefinitionVersion",
        "greengrass:getServiceRoleForAccount",
        "greengrass:getSubscriptionDefinition",
        "greengrass:getSubscriptionDefinitionVersion",
        "greengrass:listClientDevicesAssociatedWithCoreDevice",
        "greengrass:listComponents",
        "greengrass:listComponentVersions",
        "greengrass:listCoreDefinitions",
        "greengrass:listCoreDefinitionVersions",
        "greengrass:listCoreDevices",
        "greengrass:listDeployments",
        "greengrass:listEffectiveDeployments",
        "greengrass:listInstalledComponents",
        "greengrass:listDeviceDefinitions",
        "greengrass:listDeviceDefinitionVersions",
        "greengrass:listFunctionDefinitions",
        "greengrass:listFunctionDefinitionVersions",
        "greengrass:listGroups",
        "greengrass:listGroupVersions",
        "greengrass:listLoggerDefinitions",
        "greengrass:listLoggerDefinitionVersions",
        "greengrass:listResourceDefinitions",
        "greengrass:listResourceDefinitionVersions",
        "greengrass:listSubscriptionDefinitions",
        "greengrass:listSubscriptionDefinitionVersions",
        "guardduty:describeMalwareScans",
        "guardduty:describePublishingDestination",
        "guardduty:getCoverageStatistics",
        "guardduty:getDetector",
        "guardduty:getFilter",
        "guardduty:getFindings",
        "guardduty:getFindingsStatistics",
        "guardduty:getInvitationsCount",
        "guardduty:getIPSet",
        "guardduty:getMalwareProtectionPlan",
        "guardduty:getMalwareScan",
        "guardduty:getMalwareScanSettings",
        "guardduty:getMasterAccount",
        "guardduty:getMemberDetectors",
        "guardduty:getMembers",
        "guardduty:getOrganizationStatistics",
        "guardduty:getRemainingFreeTrialDays",
        "guardduty:getThreatEntitySet",
        "guardduty:getThreatIntelSet",
```

```
        "guardduty:getTrustedEntitySet",
        "guardduty:listCoverage",
        "guardduty:listDetectors",
        "guardduty:listFilters",
        "guardduty:listFindings",
        "guardduty:listInvitations",
        "guardduty:listIPSets",
        "guardduty:listMalwareProtectionPlans",
        "guardduty:listMalwareScans",
        "guardduty:listMembers",
        "guardduty:listThreatIntelSets",
        "health:describeAffectedAccountsForOrganization",
        "health:describeAffectedEntities",
        "health:describeAffectedEntitiesForOrganization",
        "health:describeEntityAggregates",
        "health:describeEntityAggregatesForOrganization",
        "health:describeEventAggregates",
        "health:describeEventDetails",
        "health:describeEventDetailsForOrganization",
        "health:describeEvents",
        "health:describeEventsForOrganization",
        "health:describeEventTypes",
        "health:describeHealthServiceStatusForOrganization",
        "iam:getAccessKeyLastUsed",
        "iam:getAccountAuthorizationDetails",
        "iam:getAccountPasswordPolicy",
        "iam:getAccountSummary",
        "iam:getContextKeysForCustomPolicy",
        "iam:getContextKeysForPrincipalPolicy",
        "iam:getCredentialReport",
        "iam:getGroup",
        "iam:getGroupPolicy",
        "iam:getInstanceProfile",
        "iam:getLoginProfile",
        "iam:getMFADevice",
        "iam:getOpenIDConnectProvider",
        "iam:getPolicy",
        "iam:getPolicyVersion",
        "iam:getRole",
        "iam:getRolePolicy",
        "iam:getSAMLProvider",
        "iam:getServerCertificate",
        "iam:getServiceLinkedRoleDeletionStatus",
        "iam:getSSHPublicKey",
```

```
        "iam:getUser",
        "iam:getUserPolicy",
        "iam:listAccessKeys",
        "iam:listAccountAliases",
        "iam:listAttachedGroupPolicies",
        "iam:listAttachedRolePolicies",
        "iam:listAttachedUserPolicies",
        "iam:listEntitiesForPolicy",
        "iam:listGroupPolicies",
        "iam:listGroups",
        "iam:listGroupsForUser",
        "iam:listInstanceProfiles",
        "iam:listInstanceProfilesForRole",
        "iam:listMFADevices",
        "iam:listOpenIDConnectProviders",
        "iam:listPolicies",
        "iam:listPolicyVersions",
        "iam:listRolePolicies",
        "iam:listRoles",
        "iam:listSAMLProviders",
        "iam:listServerCertificates",
        "iam:listServiceSpecificCredentials",
        "iam:listSigningCertificates",
        "iam:listSSHPublicKeys",
        "iam:listUserPolicies",
        "iam:listUsers",
        "iam:listVirtualMFADevices",
        "iam:simulateCustomPolicy",
        "iam:simulatePrincipalPolicy",
        "identitystore:describeGroup",
        "identitystore:describeGroupMembership",
        "identitystore:describeUser",
        "identitystore:getGroupId",
        "identitystore:getGroupMembershipId",
        "identitystore:getUserId",
        "identitystore:isMemberInGroups",
        "identitystore:listGroupMemberships",
        "identitystore:listGroupMembershipsForMember",
        "identitystore:listGroups",
        "identitystore:listUsers",
        "imagebuilder:getComponent",
        "imagebuilder:getComponentPolicy",
        "imagebuilder:getContainerRecipe",
        "imagebuilder:getContainerRecipePolicy",
```

```
        "imagebuilder:getDistributionConfiguration",
        "imagebuilder:getImage",
        "imagebuilder:getImagePipeline",
        "imagebuilder:getImagePolicy",
        "imagebuilder:getImageRecipe",
        "imagebuilder:getImageRecipePolicy",
        "imagebuilder:getInfrastructureConfiguration",
        "imagebuilder:getLifecycleExecution",
        "imagebuilder:getLifecyclePolicy",
        "imagebuilder:getWorkflow",
        "imagebuilder:getWorkflowExecution",
        "imagebuilder:getWorkflowStepExecution",
        "imagebuilder:listComponentBuildVersions",
        "imagebuilder:listComponents",
        "imagebuilder:listContainerRecipes",
        "imagebuilder:listDistributionConfigurations",
        "imagebuilder:listImageBuildVersions",
        "imagebuilder:listImagePipelineImages",
        "imagebuilder:listImagePipelines",
        "imagebuilder:listImageRecipes",
        "imagebuilder:listImages",
        "imagebuilder:listImageScanFindingAggregations",
        "imagebuilder:listInfrastructureConfigurations",
        "imagebuilder:listLifecycleExecutionResources",
        "imagebuilder:listLifecycleExecutions",
        "imagebuilder:listLifecyclePolicies",
        "imagebuilder:listTagsForResource",
        "imagebuilder:listWorkflowBuildVersions",
        "imagebuilder:listWorkflowExecutions",
        "imagebuilder:listWorkflows",
        "imagebuilder:listWaitingWorkflowSteps",
        "imagebuilder:listWorkflowStepExecutions",
        "inspector-scan:scanSbom",
        "inspector:describeAssessmentRuns",
        "inspector:describeAssessmentTargets",
        "inspector:describeAssessmentTemplates",
        "inspector:describeCrossAccountAccessRole",
        "inspector:describeResourceGroups",
        "inspector:describeRulesPackages",
        "inspector:getTelemetryMetadata",
        "inspector:listAssessmentRunAgents",
        "inspector:listAssessmentRuns",
        "inspector:listAssessmentTargets",
        "inspector:listAssessmentTemplates",
```

```
        "inspector:listEventSubscriptions",
        "inspector:listRulesPackages",
        "inspector:listTagsForResource",
        "inspector2:batchGetAccountStatus",
        "inspector2:batchGetFreeTrialInfo",
        "inspector2:describeOrganizationConfiguration",
        "inspector2:getConfiguration",
        "inspector2:getDelegatedAdminAccount",
        "inspector2:getEc2DeepInspectionConfiguration",
        "inspector2:getMember",
        "inspector2:getSbomExport",
        "inspector2:listCisScanConfigurations",
        "inspector2:listCisScanResultsAggregatedByChecks",
        "inspector2:listCisScanResultsAggregatedByTargetResource",
        "inspector2:listCisScans",
        "inspector2:listCoverage",
        "inspector2:listDelegatedAdminAccounts",
        "inspector2:listFilters",
        "inspector2:listFindings",
        "inspector2:listMembers",
        "inspector2:listUsageTotals",
        "internetmonitor:getHealthEvent",
        "internetmonitor:getMonitor",
        "internetmonitor:listHealthEvents",
        "internetmonitor:listMonitors",
        "invoicing:batchGetInvoiceProfile",
        "invoicing:listInvoiceSummaries",
        "invoicing:listInvoiceUnits",
        "iot:describeAuthorizer",
        "iot:describeCACertificate",
        "iot:describeCertificate",
        "iot:describeDefaultAuthorizer",
        "iot:describeDomainConfiguration",
        "iot:describeEndpoint",
        "iot:describeIndex",
        "iot:describeJobExecution",
        "iot:describeThing",
        "iot:describeThingGroup",
        "iot:describeTunnel",
        "iot:getEffectivePolicies",
        "iot:getIndexingConfiguration",
        "iot:getLoggingOptions",
        "iot:getPolicy",
        "iot:getPolicyVersion",
```

```
        "iot:getTopicRule",
        "iot:getV2LoggingOptions",
        "iot:listAttachedPolicies",
        "iot:listAuthorizers",
        "iot:listCACertificates",
        "iot:listCertificates",
        "iot:listCertificatesByCA",
        "iot:listCommandExecutions",
        "iot:listCommands",
        "iot:listDomainConfigurations",
        "iot:listJobExecutionsForJob",
        "iot:listJobExecutionsForThing",
        "iot:listJobs",
        "iot:listNamedShadowsForThing",
        "iot:listOutgoingCertificates",
        "iot:listPackages",
        "iot:listPackageVersions",
        "iot:listPolicies",
        "iot:listPolicyPrincipals",
        "iot:listPolicyVersions",
        "iot:listPrincipalPolicies",
        "iot:listPrincipalThings",
        "iot:listRoleAliases",
        "iot:listTargetsForPolicy",
        "iot:listThingGroups",
        "iot:listThingGroupsForThing",
        "iot:listThingPrincipals",
        "iot:listThingRegistrationTasks",
        "iot:listThings",
        "iot:listThingsInThingGroup",
        "iot:listThingTypes",
        "iot:listTopicRules",
        "iot:listTunnels",
        "iot:listV2LoggingLevels",
        "iotevents:describeDetector",
        "iotevents:describeDetectorModel",
        "iotevents:describeInput",
        "iotevents:describeLoggingOptions",
        "iotevents:listDetectorModels",
        "iotevents:listDetectorModelVersions",
        "iotevents:listDetectors",
        "iotevents:listInputs",
        "iotfleetwise:getCampaign",
        "iotfleetwise:getDecoderManifest",
```

```
        "iotfleetwise:getEncryptionConfiguration",
        "iotfleetwise:getFleet",
        "iotfleetwise:getLoggingOptions",
        "iotfleetwise:getModelManifest",
        "iotfleetwise:getRegisterAccountStatus",
        "iotfleetwise:getSignalCatalog",
        "iotfleetwise:getStateTemplate",
        "iotfleetwise:getVehicle",
        "iotfleetwise:getVehicleStatus",
        "iotfleetwise:listCampaigns",
        "iotfleetwise:listDecoderManifestNetworkInterfaces",
        "iotfleetwise:listDecoderManifests",
        "iotfleetwise:listDecoderManifestSignals",
        "iotfleetwise:listFleets",
        "iotfleetwise:listFleetsForVehicle",
        "iotfleetwise:listModelManifestNodes",
        "iotfleetwise:listModelManifests",
        "iotfleetwise:listSignalCatalogNodes",
        "iotfleetwise:listSignalCatalogs",
        "iotfleetwise:listStateTemplates",
        "iotfleetwise:listVehicles",
        "iotfleetwise:listVehiclesInFleet",
        "iotsitewise:describeAccessPolicy",
        "iotsitewise:describeAsset",
        "iotsitewise:describeAssetModel",
        "iotsitewise:describeAssetProperty",
        "iotsitewise:describeDashboard",
        "iotsitewise:describeGateway",
        "iotsitewise:describeGatewayCapabilityConfiguration",
        "iotsitewise:describeLoggingOptions",
        "iotsitewise:describePortal",
        "iotsitewise:describeProject",
        "iotsitewise:listAccessPolicies",
        "iotsitewise:listAssetModels",
        "iotsitewise:listAssets",
        "iotsitewise:listAssociatedAssets",
        "iotsitewise:listDashboards",
        "iotsitewise:listGateways",
        "iotsitewise:listPortals",
        "iotsitewise:listProjectAssets",
        "iotsitewise:listProjects",
        "iottwinmaker:getComponentType",
        "iottwinmaker:getEntity",
        "iottwinmaker:getPricingPlan",
```

```
        "iottwinmaker:getScene",
        "iottwinmaker:getSyncJob",
        "iottwinmaker:getWorkspace",
        "iottwinmaker:listComponentTypes",
        "iottwinmaker:listEntities",
        "iottwinmaker:listScenes",
        "iottwinmaker:listSyncJobs",
        "iottwinmaker:listSyncResources",
        "iottwinmaker:listWorkspaces",
        "iotwireless:getDestination",
        "iotwireless:getDeviceProfile",
        "iotwireless:getPartnerAccount",
        "iotwireless:getServiceEndpoint",
        "iotwireless:getServiceProfile",
        "iotwireless:getWirelessDevice",
        "iotwireless:getWirelessDeviceStatistics",
        "iotwireless:getWirelessGateway",
        "iotwireless:getWirelessGatewayCertificate",
        "iotwireless:getWirelessGatewayFirmwareInformation",
        "iotwireless:getWirelessGatewayStatistics",
        "iotwireless:getWirelessGatewayTask",
        "iotwireless:getWirelessGatewayTaskDefinition",
        "iotwireless:listDestinations",
        "iotwireless:listDeviceProfiles",
        "iotwireless:listPartnerAccounts",
        "iotwireless:listServiceProfiles",
        "iotwireless:listTagsForResource",
        "iotwireless:listWirelessDevices",
        "iotwireless:listWirelessGateways",
        "iotwireless:listWirelessGatewayTaskDefinitions",
        "ivs:getChannel",
        "ivs:getRecordingConfiguration",
        "ivs:getStream",
        "ivs:getStreamSession",
        "ivs:listChannels",
        "ivs:listPlaybackKeyPairs",
        "ivs:listRecordingConfigurations",
        "ivs:listStreamKeys",
        "ivs:listStreams",
        "ivs:listStreamSessions",
        "kafka:describeCluster",
        "kafka:describeClusterOperation",
        "kafka:describeClusterOperationV2",
        "kafka:describeClusterV2",
```

```
        "kafka:describeConfiguration",
        "kafka:describeConfigurationRevision",
        "kafka:describeReplicator",
        "kafka:describeTopic",
        "kafka:describeTopicPartitions",
        "kafka:describeVpcConnection",
        "kafka:getBootstrapBrokers",
        "kafka:getClusterPolicy",
        "kafka:getCompatibleKafkaVersions",
        "kafka:listClientVpcConnections",
        "kafka:listClusterOperations",
        "kafka:listClusterOperationsV2",
        "kafka:listClusters",
        "kafka:listClustersV2",
        "kafka:listConfigurationRevisions",
        "kafka:listConfigurations",
        "kafka:listNodes",
        "kafka:listReplicators",
        "kafka:listScramSecrets",
        "kafka:listTagsForResource",
        "kafka:listTopics",
        "kafka:listVpcConnections",
        "kafkaconnect:describeConnector",
        "kafkaconnect:describeCustomPlugin",
        "kafkaconnect:describeWorkerConfiguration",
        "kafkaconnect:listConnectors",
        "kafkaconnect:listCustomPlugins",
        "kafkaconnect:listWorkerConfigurations",
        "kendra:describeAccessControlConfiguration",
        "kendra:describeDataSource",
        "kendra:describeExperience",
        "kendra:describeFaq",
        "kendra:describeFeaturedResultsSet",
        "kendra:describeIndex",
        "kendra:describePrincipalMapping",
        "kendra:describeQuerySuggestionsBlockList",
        "kendra:describeQuerySuggestionsConfig",
        "kendra:describeThesaurus",
        "kendra:listAccessControlConfigurations",
        "kendra:listDataSourceSyncJobs",
        "kendra:listDataSources",
        "kendra:listEntityPersonas",
        "kendra:listExperienceEntities",
        "kendra:listExperiences",
```

```
        "kendra:listFaqs",
        "kendra:listFeaturedResultsSets",
        "kendra:listIndices",
        "kendra:listQuerySuggestionsBlockLists",
        "kendra:listThesauri",
        "kinesis:describeStream",
        "kinesis:describeStreamConsumer",
        "kinesis:describeStreamSummary",
        "kinesis:listShards",
        "kinesis:listStreamConsumers",
        "kinesis:listStreams",
        "kinesis:listTagsForStream",
        "kinesisanalytics:describeApplication",
        "kinesisanalytics:describeApplicationOperation",
        "kinesisanalytics:describeApplicationSnapshot",
        "kinesisanalytics:listApplicationOperations",
        "kinesisanalytics:listApplications",
        "kinesisanalytics:listApplicationSnapshots",
        "kinesisanalytics:listApplicationVersions",
        "kinesisvideo:describeImageGenerationConfiguration",
        "kinesisvideo:describeEdgeConfiguration",
        "kinesisvideo:describeMappedResourceConfiguration",
        "kinesisvideo:describeMediaStorageConfiguration",
        "kinesisvideo:describeNotificationConfiguration",
        "kinesisvideo:describeSignalingChannel",
        "kinesisvideo:describeStream",
        "kinesisvideo:getDataEndpoint",
        "kinesisvideo:getIceServerConfig",
        "kinesisvideo:getSignalingChannelEndpoint",
        "kinesisvideo:listSignalingChannels",
        "kinesisvideo:listEdgeAgentConfigurations",
        "kinesisvideo:listStreams",
        "kms:describeCustomKeyStores",
        "kms:describeKey",
        "kms:getKeyPolicy",
        "kms:getKeyRotationStatus",
        "kms:listAliases",
        "kms:listGrants",
        "kms:listKeyPolicies",
        "kms:listKeyRotations",
        "kms:listKeys",
        "kms:listResourceTags",
        "kms:listRetirableGrants",
        "lakeformation:describeLakeFormationIdentityCenterConfiguration",
```

```
        "lakeformation:describeResource",
        "lakeformation:describeTransaction",
        "lakeformation:getDataLakePrincipal",
        "lakeformation:getDataLakeSettings",
        "lakeformation:getEffectivePermissionsForPath",
        "lakeformation:getLFTag",
        "lakeformation:getLFTagExpression",
        "lakeformation:getQueryState",
        "lakeformation:getQueryStatistics",
        "lakeformation:getResourceLFTags",
        "lakeformation:listLFTagExpressions",
        "lakeformation:listLFTags",
        "lakeformation:listLakeFormationOptIns",
        "lakeformation:listPermissions",
        "lakeformation:listResources",
        "lakeformation:searchDatabasesByLFTags",
        "lakeformation:searchTablesByLFTags",
        "lambda:getAccountSettings",
        "lambda:getAlias",
        "lambda:getCodeSigningConfig",
        "lambda:getDurableExecution",
        "lambda:getDurableExecutionHistory",
        "lambda:getDurableExecutionState",
        "lambda:getEventSourceMapping",
        "lambda:getFunction",
        "lambda:getFunctionCodeSigningConfig",
        "lambda:getFunctionConcurrency",
        "lambda:getFunctionConfiguration",
        "lambda:getFunctionEventInvokeConfig",
        "lambda:getFunctionRecursionConfig",
        "lambda:getFunctionScalingConfig",
        "lambda:getFunctionUrlConfig",
        "lambda:getLayerVersion",
        "lambda:getLayerVersionPolicy",
        "lambda:getMicrovm",
        "lambda:getMicrovmImage",
        "lambda:getMicrovmImageBuild",
        "lambda:getMicrovmImageVersion",
        "lambda:getPolicy",
        "lambda:getCapacityProvider",
        "lambda:getProvisionedConcurrencyConfig",
        "lambda:getRuntimeManagementConfig",
        "lambda:listAliases",
        "lambda:listCapacityProviders",
```

```
        "lambda:listCodeSigningConfigs",
        "lambda:listDurableExecutionsByFunction",
        "lambda:listEventSourceMappings",
        "lambda:listFunctionEventInvokeConfigs",
        "lambda:listFunctions",
        "lambda:listFunctionsByCodeSigningConfig",
        "lambda:listFunctionUrlConfigs",
        "lambda:listFunctionVersionsByCapacityProvider",
        "lambda:listLayers",
        "lambda:listLayerVersions",
        "lambda:listManagedMicrovmImages",
        "lambda:listManagedMicrovmImageVersions",
        "lambda:listMicrovmImageBuilds",
        "lambda:listMicrovmImages",
        "lambda:listMicrovmImageVersions",
        "lambda:listMicrovms",
        "lambda:listProvisionedConcurrencyConfigs",
        "lambda:listTags",
        "lambda:listVersionsByFunction",
        "launchwizard:describeProvisionedApp",
        "launchwizard:describeProvisioningEvents",
        "launchwizard:listDeploymentEvents",
        "launchwizard:listDeployments",
        "launchwizard:listProvisionedApps",
        "lex:describeBot",
        "lex:describeBotAlias",
        "lex:describeBotLocale",
        "lex:describeBotRecommendation",
        "lex:describeBotVersion",
        "lex:describeCustomVocabularyMetadata",
        "lex:describeExport",
        "lex:describeImport",
        "lex:describeIntent",
        "lex:describeResourcePolicy",
        "lex:describeSlot",
        "lex:describeSlotType",
        "lex:getBot",
        "lex:getBotAlias",
        "lex:getBotAliases",
        "lex:getBotChannelAssociation",
        "lex:getBotChannelAssociations",
        "lex:getBots",
        "lex:getBotVersions",
        "lex:getBuiltinIntent",
```

```
        "lex:getBuiltinIntents",
        "lex:getBuiltinSlotTypes",
        "lex:getIntent",
        "lex:getIntents",
        "lex:getIntentVersions",
        "lex:getSlotType",
        "lex:getSlotTypes",
        "lex:getSlotTypeVersions",
        "lex:listBotAliases",
        "lex:listBotLocales",
        "lex:listBotRecommendations",
        "lex:listBots",
        "lex:listBotVersions",
        "lex:listExports",
        "lex:listImports",
        "lex:listIntents",
        "lex:listRecommendedIntents",
        "lex:listSlots",
        "lex:listSlotTypes",
        "license-manager:getGrant",
        "license-manager:getLicense",
        "license-manager:getLicenseConfiguration",
        "license-manager:getLicenseConversionTask",
        "license-manager:getLicenseManagerReportGenerator",
        "license-manager:getLicenseUsage",
        "license-manager:getServiceSettings",
        "license-manager:listAssociationsForLicenseConfiguration",
        "license-manager:listDistributedGrants",
        "license-manager:listFailuresForLicenseConfigurationOperations",
        "license-manager:listLicenseConfigurations",
        "license-manager:listLicenseConversionTasks",
        "license-manager:listLicenseManagerReportGenerators",
        "license-manager:listLicenses",
        "license-manager:listLicenseSpecificationsForResource",
        "license-manager:listLicenseVersions",
        "license-manager:listReceivedGrants",
        "license-manager:listReceivedGrantsForOrganization",
        "license-manager:listReceivedLicenses",
        "license-manager:listReceivedLicensesForOrganization",
        "license-manager:listResourceInventory",
        "license-manager:listTokens",
        "license-manager:listUsageForLicenseConfiguration",
        "license-manager-linux-subscriptions:getRegisteredSubscriptionProvider",
        "license-manager-linux-subscriptions:getServiceSettings",
```

```
        "license-manager-linux-subscriptions:listLinuxSubscriptionInstances",
        "license-manager-linux-subscriptions:listLinuxSubscriptions",
        "license-manager-linux-subscriptions:listRegisteredSubscriptionProviders",
        "license-manager-user-subscriptions:listIdentityProviders",
        "license-manager-user-subscriptions:listInstances",
        "license-manager-user-subscriptions:listLicenseServerEndpoints",
        "license-manager-user-subscriptions:listProductSubscriptions",
        "license-manager-user-subscriptions:listUserAssociations",
        "lightsail:getActiveNames",
        "lightsail:getAlarms",
        "lightsail:getAutoSnapshots",
        "lightsail:getBlueprints",
        "lightsail:getBucketBundles",
        "lightsail:getBucketMetricData",
        "lightsail:getBuckets",
        "lightsail:getBundles",
        "lightsail:getCertificates",
        "lightsail:getContainerImages",
        "lightsail:getContainerServiceDeployments",
        "lightsail:getContainerServiceMetricData",
        "lightsail:getContainerServicePowers",
        "lightsail:getContainerServices",
        "lightsail:getDisk",
        "lightsail:getDisks",
        "lightsail:getDiskSnapshot",
        "lightsail:getDiskSnapshots",
        "lightsail:getDistributionBundles",
        "lightsail:getDistributionMetricData",
        "lightsail:getDistributions",
        "lightsail:getDomain",
        "lightsail:getDomains",
        "lightsail:getExportSnapshotRecords",
        "lightsail:getInstance",
        "lightsail:getInstanceMetricData",
        "lightsail:getInstancePortStates",
        "lightsail:getInstances",
        "lightsail:getInstanceSnapshot",
        "lightsail:getInstanceSnapshots",
        "lightsail:getInstanceState",
        "lightsail:getKeyPair",
        "lightsail:getKeyPairs",
        "lightsail:getLoadBalancer",
        "lightsail:getLoadBalancerMetricData",
        "lightsail:getLoadBalancers",
```

```
        "lightsail:getLoadBalancerTlsCertificates",
        "lightsail:getOperation",
        "lightsail:getOperations",
        "lightsail:getOperationsForResource",
        "lightsail:getRegions",
        "lightsail:getRelationalDatabase",
        "lightsail:getRelationalDatabaseMetricData",
        "lightsail:getRelationalDatabases",
        "lightsail:getRelationalDatabaseSnapshot",
        "lightsail:getRelationalDatabaseSnapshots",
        "lightsail:getStaticIp",
        "lightsail:getStaticIps",
        "lightsail:isVpcPeered",
        "logs:describeAccountPolicies",
        "logs:describeDeliveries",
        "logs:describeDeliveryDestinations",
        "logs:describeDeliverySources",
        "logs:describeDestinations",
        "logs:describeExportTasks",
        "logs:describeFieldIndexes",
        "logs:describeIndexPolicies",
        "logs:describeLogGroups",
        "logs:describeLogStreams",
        "logs:describeMetricFilters",
        "logs:describeQueries",
        "logs:describeQueryDefinitions",
        "logs:describeResourcePolicies",
        "logs:describeSubscriptionFilters",
        "logs:getDataProtectionPolicy",
        "logs:getDelivery",
        "logs:getDeliveryDestination",
        "logs:getDeliveryDestinationPolicy",
        "logs:getDeliverySource",
        "logs:getIntegration",
        "logs:getLogAnomalyDetector",
        "logs:getLogDelivery",
        "logs:getLogGroupFields",
        "logs:getTransformer",
        "logs:listAnomalies",
        "logs:listIntegrations",
        "logs:listLogAnomalyDetectors",
        "logs:listLogDeliveries",
        "logs:listLogGroups",
        "logs:listLogGroupsForQuery",
```

```
        "logs:testMetricFilter",
        "lookoutequipment:describeDataIngestionJob",
        "lookoutequipment:describeDataset",
        "lookoutequipment:describeInferenceScheduler",
        "lookoutequipment:describeModel",
        "lookoutequipment:listDataIngestionJobs",
        "lookoutequipment:listDatasets",
        "lookoutequipment:listInferenceExecutions",
        "lookoutequipment:listInferenceSchedulers",
        "lookoutequipment:listModels",
        "m2:getApplication",
        "m2:getApplicationVersion",
        "m2:getBatchJobExecution",
        "m2:getDataSetDetails",
        "m2:getDataSetImportTask",
        "m2:getDeployment",
        "m2:getEnvironment",
        "m2:listApplications",
        "m2:listApplicationVersions",
        "m2:listBatchJobDefinitions",
        "m2:listBatchJobExecutions",
        "m2:listDataSetImportHistory",
        "m2:listDataSets",
        "m2:listDeployments",
        "m2:listEngineVersions",
        "m2:listEnvironments",
        "machinelearning:describeBatchPredictions",
        "machinelearning:describeDataSources",
        "machinelearning:describeEvaluations",
        "machinelearning:describeMLModels",
        "machinelearning:getBatchPrediction",
        "machinelearning:getDataSource",
        "machinelearning:getEvaluation",
        "machinelearning:getMLModel",
        "macie2:describeBuckets",
        "macie2:describeClassificationJob",
        "macie2:getAdministratorAccount",
        "macie2:getAllowList",
        "macie2:getAutomatedDiscoveryConfiguration",
        "macie2:getClassificationExportConfiguration",
        "macie2:getClassificationScope",
        "macie2:getCustomDataIdentifier",
        "macie2:getFindings",
        "macie2:getFindingsFilter",
```

```
        "macie2:getFindingsPublicationConfiguration",
        "macie2:getFindingStatistics",
        "macie2:getMacieSession",
        "macie2:getMember",
        "macie2:getResourceProfile",
        "macie2:getRevealConfiguration",
        "macie2:getSensitivityInspectionTemplate",
        "macie2:getUsageStatistics",
        "macie2:listAllowLists",
        "macie2:listAutomatedDiscoveryAccounts",
        "macie2:listClassificationJobs",
        "macie2:listClassificationScopes",
        "macie2:listCustomDataIdentifiers",
        "macie2:listFindings",
        "macie2:listFindingsFilters",
        "macie2:listMembers",
        "macie2:listSensitivityInspectionTemplates",
        "managedblockchain:getMember",
        "managedblockchain:getNetwork",
        "managedblockchain:getNode",
        "managedblockchain:listMembers",
        "managedblockchain:listNetworks",
        "managedblockchain:listNodes",
        "mediaconnect:describeFlow",
        "mediaconnect:listEntitlements",
        "mediaconnect:listFlows",
        "mediaconvert:describeEndpoints",
        "mediaconvert:getJob",
        "mediaconvert:getJobTemplate",
        "mediaconvert:getPreset",
        "mediaconvert:getQueue",
        "mediaconvert:listJobs",
        "mediaconvert:listJobTemplates",
        "medialive:describeChannel",
        "medialive:describeInput",
        "medialive:describeInputDevice",
        "medialive:describeInputSecurityGroup",
        "medialive:describeMultiplex",
        "medialive:describeOffering",
        "medialive:describeReservation",
        "medialive:describeSchedule",
        "medialive:getCloudWatchAlarmTemplate",
        "medialive:getCloudWatchAlarmTemplateGroup",
        "medialive:getEventBridgeRuleTemplate",
```

```
        "medialive:getEventBridgeRuleTemplateGroup",
        "medialive:getSignalMap",
        "medialive:listChannels",
        "medialive:listCloudWatchAlarmTemplateGroups",
        "medialive:listCloudWatchAlarmTemplates",
        "medialive:listEventBridgeRuleTemplateGroups",
        "medialive:listEventBridgeRuleTemplates",
        "medialive:listInputDevices",
        "medialive:listInputs",
        "medialive:listInputSecurityGroups",
        "medialive:listMultiplexes",
        "medialive:listOfferings",
        "medialive:listReservations",
        "medialive:listSignalMaps",
        "mediapackage:describeChannel",
        "mediapackage:describeOriginEndpoint",
        "mediapackage:listChannels",
        "mediapackage:listOriginEndpoints",
        "mediastore:describeContainer",
        "mediastore:getContainerPolicy",
        "mediastore:getCorsPolicy",
        "mediastore:listContainers",
        "mediatailor:getPlaybackConfiguration",
        "mediatailor:listPlaybackConfigurations",
        "medical-imaging:getDatastore",
        "medical-imaging:listDatastores",
        "memorydb:describeReservedNodesOfferings",
        "memorydb:listAllowedNodeTypeUpdates",
        "mgn:describeJobLogItems",
        "mgn:describeJobs",
        "mgn:describeLaunchConfigurationTemplates",
        "mgn:describeReplicationConfigurationTemplates",
        "mgn:describeSourceServers",
        "mgn:describeVcenterClients",
        "mgn:getLaunchConfiguration",
        "mgn:getReplicationConfiguration",
        "mgn:listApplications",
        "mgn:listSourceServerActions",
        "mgn:listTemplateActions",
        "mgn:listWaves",
        "mobiletargeting:getAdmChannel",
        "mobiletargeting:getApnsChannel",
        "mobiletargeting:getApnsSandboxChannel",
        "mobiletargeting:getApnsVoipChannel",
```

```
        "mobiletargeting:getApnsVoipSandboxChannel",
        "mobiletargeting:getApp",
        "mobiletargeting:getApplicationSettings",
        "mobiletargeting:getApps",
        "mobiletargeting:getBaiduChannel",
        "mobiletargeting:getCampaign",
        "mobiletargeting:getCampaignActivities",
        "mobiletargeting:getCampaigns",
        "mobiletargeting:getCampaignVersion",
        "mobiletargeting:getCampaignVersions",
        "mobiletargeting:getEmailChannel",
        "mobiletargeting:getEndpoint",
        "mobiletargeting:getEventStream",
        "mobiletargeting:getExportJob",
        "mobiletargeting:getExportJobs",
        "mobiletargeting:getGcmChannel",
        "mobiletargeting:getImportJob",
        "mobiletargeting:getImportJobs",
        "mobiletargeting:getJourney",
        "mobiletargeting:getJourneyExecutionActivityMetrics",
        "mobiletargeting:getJourneyExecutionMetrics",
        "mobiletargeting:getJourneyRunExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionMetrics",
        "mobiletargeting:getJourneyRuns",
        "mobiletargeting:getSegment",
        "mobiletargeting:getSegmentImportJobs",
        "mobiletargeting:getSegments",
        "mobiletargeting:getSegmentVersion",
        "mobiletargeting:getSegmentVersions",
        "mobiletargeting:getSmsChannel",
        "mobiletargeting:listJourneys",
        "mobiletargeting:phoneNumberValidate",
        "mpa:getApprovalTeam",
        "mpa:getSession",
        "mpa:listApprovalTeams",
        "mq:describeBrokerInstanceOptions",
        "mq:describeBroker",
        "mq:describeConfiguration",
        "mq:describeConfigurationRevision",
        "mq:describeUser",
        "mq:listBrokers",
        "mq:listConfigurationRevisions",
        "mq:listConfigurations",
        "mq:listUsers",
```

```
            "network-firewall:describeFirewall",
            "network-firewall:describeFirewallPolicy",
            "network-firewall:describeFlowOperation",
            "network-firewall:describeLoggingConfiguration",
            "network-firewall:describeResourcePolicy",
            "network-firewall:describeRuleGroup",
            "network-firewall:describeRuleGroupMetadata",
            "network-firewall:describeTlsInspectionConfiguration",
            "network-firewall:describeVpcEndpointAssociation",
            "network-firewall:listAnalysisReports",
            "network-firewall:listFirewallPolicies",
            "network-firewall:listFirewalls",
            "network-firewall:listFlowOperationResults",
            "network-firewall:listFlowOperations",
            "network-firewall:listRuleGroups",
            "network-firewall:listTlsInspectionConfigurations",
            "network-firewall:listVpcEndpointAssociations",
            "networkflowmonitor:getMonitor",
            "networkflowmonitor:getScope",
            "networkflowmonitor:listMonitors",
            "networkflowmonitor:listScopes",
            "networkmanager:describeGlobalNetworks",
            "networkmanager:getConnectAttachment",
            "networkmanager:getConnections",
            "networkmanager:getConnectPeer",
            "networkmanager:getConnectPeerAssociations",
            "networkmanager:getCoreNetwork",
            "networkmanager:getCoreNetworkChangeEvents",
            "networkmanager:getCoreNetworkChangeSet",
            "networkmanager:getCoreNetworkPolicy",
            "networkmanager:getCustomerGatewayAssociations",
            "networkmanager:getDevices",
            "networkmanager:getDirectConnectGatewayAttachment",
            "networkmanager:getLinkAssociations",
            "networkmanager:getLinks",
            "networkmanager:getNetworkResourceCounts",
            "networkmanager:getNetworkResourceRelationships",
            "networkmanager:getNetworkResources",
            "networkmanager:getNetworkRoutes",
            "networkmanager:getNetworkTelemetry",
            "networkmanager:getResourcePolicy",
            "networkmanager:getRouteAnalysis",
            "networkmanager:getSites",
            "networkmanager:getSiteToSiteVpnAttachment",
```

```
        "networkmanager:getTransitGatewayConnectPeerAssociations",
        "networkmanager:getTransitGatewayPeering",
        "networkmanager:getTransitGatewayRegistrations",
        "networkmanager:getTransitGatewayRouteTableAttachment",
        "networkmanager:getVpcAttachment",
        "networkmanager:listAttachments",
        "networkmanager:listConnectPeers",
        "networkmanager:listCoreNetworkPolicyVersions",
        "networkmanager:listCoreNetworks",
        "networkmanager:listOrganizationServiceAccessStatus",
        "networkmanager:listPeerings",
        "networkmanager:listTagsForResource",
        "networkmonitor:getMonitor",
        "networkmonitor:getProbe",
        "networkmonitor:listMonitors",
        "notifications-contacts:getEmailContact",
        "notifications-contacts:listEmailContacts",
        "notifications:getEventRule",
        "notifications:getNotificationConfiguration",
        "notifications:getNotificationEvent",
        "notifications:listChannels",
        "notifications:listEventRules",
        "notifications:listNotificationConfigurations",
        "notifications:listNotificationEvents",
        "notifications:listNotificationHubs",
        "oam:getLink",
        "oam:getSink",
        "oam:getSinkPolicy",
        "oam:listAttachedLinks",
        "oam:listLinks",
        "oam:listSinks",
        "observabilityadmin:getTelemetryEvaluationStatus",
        "observabilityadmin:getTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:listResourceTelemetry",
        "observabilityadmin:listResourceTelemetryForOrganization",
        "odb:getCloudAutonomousVmCluster",
        "odb:getCloudExadataInfrastructure",
        "odb:getCloudExadataInfrastructureUnallocatedResources",
        "odb:getCloudVmCluster",
        "odb:getOciOnboardingStatus",
        "odb:getOdbNetwork",
        "odb:getOdbPeeringConnection",
        "odb:listCloudAutonomousVmClusters",
        "odb:listCloudExadataInfrastructures",
```

```
        "odb:listCloudVmClusters",
        "odb:listOdbNetworks",
        "odb:listOdbPeeringConnections",
        "omics:getAnnotationImportJob",
        "omics:getAnnotationStore",
        "omics:getAnnotationStoreVersion",
        "omics:getReadSetActivationJob",
        "omics:getReadSetExportJob",
        "omics:getReadSetImportJob",
        "omics:getReadSetMetadata",
        "omics:getReference",
        "omics:getReferenceImportJob",
        "omics:getReferenceMetadata",
        "omics:getReferenceStore",
        "omics:getRun",
        "omics:getRunCache",
        "omics:getRunGroup",
        "omics:getRunTask",
        "omics:getSequenceStore",
        "omics:getShare",
        "omics:getVariantImportJob",
        "omics:getVariantStore",
        "omics:getWorkflow",
        "omics:getWorkflowVersion",
        "omics:listAnnotationImportJobs",
        "omics:listAnnotationStores",
        "omics:listAnnotationStoreVersions",
        "omics:listMultipartReadSetUploads",
        "omics:listReadSetActivationJobs",
        "omics:listReadSetExportJobs",
        "omics:listReadSetImportJobs",
        "omics:listReadSets",
        "omics:listReadSetUploadParts",
        "omics:listReferenceImportJobs",
        "omics:listReferences",
        "omics:listReferenceStores",
        "omics:listRunCaches"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup3",
```

```
      "Effect" : "Allow",
      "Action" : [
        "omics:listRunGroups",
        "omics:listRuns",
        "omics:listRunTasks",
        "omics:listSequenceStores",
        "omics:listShares",
        "omics:listVariantImportJobs",
        "omics:listVariantStores",
        "omics:listWorkflows",
        "omics:listWorkflowVersions",
        "opsworks-cm:describeAccountAttributes",
        "opsworks-cm:describeBackups",
        "opsworks-cm:describeEvents",
        "opsworks-cm:describeNodeAssociationStatus",
        "opsworks-cm:describeServers",
        "opsworks:describeAgentVersions",
        "opsworks:describeApps",
        "opsworks:describeCommands",
        "opsworks:describeDeployments",
        "opsworks:describeEcsClusters",
        "opsworks:describeElasticIps",
        "opsworks:describeElasticLoadBalancers",
        "opsworks:describeInstances",
        "opsworks:describeLayers",
        "opsworks:describeLoadBasedAutoScaling",
        "opsworks:describeMyUserProfile",
        "opsworks:describePermissions",
        "opsworks:describeRaidArrays",
        "opsworks:describeRdsDbInstances",
        "opsworks:describeServiceErrors",
        "opsworks:describeStackProvisioningParameters",
        "opsworks:describeStacks",
        "opsworks:describeStackSummary",
        "opsworks:describeTimeBasedAutoScaling",
        "opsworks:describeUserProfiles",
        "opsworks:describeVolumes",
        "opsworks:getHostnameSuggestion",
        "organizations:describeAccount",
        "organizations:describeCreateAccountStatus",
        "organizations:describeEffectivePolicy",
        "organizations:describeHandshake",
        "organizations:describeOrganization",
        "organizations:describeOrganizationalUnit",
```

```
        "organizations:describePolicy",
        "organizations:describeResourcePolicy",
        "organizations:listAccounts",
        "organizations:listAccountsForParent",
        "organizations:listAWSServiceAccessForOrganization",
        "organizations:listChildren",
        "organizations:listCreateAccountStatus",
        "organizations:listDelegatedAdministrators",
        "organizations:listDelegatedServicesForAccount",
        "organizations:listHandshakesForAccount",
        "organizations:listHandshakesForOrganization",
        "organizations:listOrganizationalUnitsForParent",
        "organizations:listParents",
        "organizations:listPolicies",
        "organizations:listPoliciesForTarget",
        "organizations:listRoots",
        "organizations:listTagsForResource",
        "organizations:listTargetsForPolicy",
        "osis:getPipeline",
        "osis:getPipelineBlueprint",
        "osis:getPipelineChangeProgress",
        "osis:listPipelineBlueprints",
        "osis:listPipelines",
        "osis:validatePipeline",
        "outposts:getCapacityTask",
        "outposts:getCatalogItem",
        "outposts:getConnection",
        "outposts:getOrder",
        "outposts:getOutpost",
        "outposts:getOutpostInstanceTypes",
        "outposts:getOutpostSupportedInstanceTypes",
        "outposts:getSite",
        "outposts:listAssets",
        "outposts:listAssetInstances",
        "outposts:listBlockingInstancesForCapacityTask",
        "outposts:listCapacityTasks",
        "outposts:listCatalogItems",
        "outposts:listOrders",
        "outposts:listOutposts",
        "outposts:listSites",
        "payment-cryptography:getAlias",
        "payment-cryptography:getKey",
        "payment-cryptography:listAliases",
        "payment-cryptography:listKeys",
```

```
        "pca-connector-ad:listConnectors",
        "pca-connector-ad:listDirectoryRegistrations",
        "pca-connector-ad:listServicePrincipalNames",
        "pca-connector-ad:listTagsForResource",
        "pca-connector-ad:listTemplateGroupAccessControlEntries",
        "pca-connector-ad:listTemplates",
        "pcs:getCluster",
        "pcs:getComputeNodeGroup",
        "pcs:getQueue",
        "pcs:listClusters",
        "pcs:listComputeNodeGroups",
        "pcs:listQueues",
        "personalize:describeAlgorithm",
        "personalize:describeBatchInferenceJob",
        "personalize:describeBatchSegmentJob",
        "personalize:describeCampaign",
        "personalize:describeDataInsightsJob",
        "personalize:describeDataset",
        "personalize:describeDatasetExportJob",
        "personalize:describeDatasetGroup",
        "personalize:describeDatasetImportJob",
        "personalize:describeEventTracker",
        "personalize:describeFeatureTransformation",
        "personalize:describeFilter",
        "personalize:describeMetricAttribution",
        "personalize:describeRecipe",
        "personalize:describeRecommender",
        "personalize:describeSchema",
        "personalize:describeSolution",
        "personalize:describeSolutionVersion",
        "personalize:getPersonalizedRanking",
        "personalize:getRecommendations",
        "personalize:getSolutionMetrics",
        "personalize:listBatchInferenceJobs",
        "personalize:listBatchSegmentJobs",
        "personalize:listCampaigns",
        "personalize:listDataInsightsJobs",
        "personalize:listDatasetExportJobs",
        "personalize:listDatasetGroups",
        "personalize:listDatasetImportJobs",
        "personalize:listDatasets",
        "personalize:listEventTrackers",
        "personalize:listMetricAttributions",
        "personalize:listRecipes",
```

```
        "personalize:listRecommenders",
        "personalize:listSchemas",
        "personalize:listSolutions",
        "personalize:listSolutionVersions",
        "pipes:describePipe",
        "pipes:listPipes",
        "pipes:listTagsForResource",
        "polly:describeVoices",
        "polly:getLexicon",
        "polly:listLexicons",
        "pricing:describeServices",
        "pricing:getAttributeValues",
        "pricing:getProducts",
        "private-networks:getDeviceIdentifier",
        "private-networks:getNetwork",
        "private-networks:getNetworkResource",
        "private-networks:listDeviceIdentifiers",
        "private-networks:listNetworkResources",
        "private-networks:listNetworks",
        "qbusiness:getApplication",
        "qbusiness:getDataSource",
        "qbusiness:getIndex",
        "qbusiness:getRetriever",
        "qbusiness:getWebExperience",
        "qbusiness:listApplications",
        "qbusiness:listDataSources",
        "qbusiness:listDataSourceSyncJobs",
        "qbusiness:listIndices",
        "qbusiness:listRetrievers",
        "qbusiness:listWebExperiences",
        "quicksight:describeAccountCustomization",
        "quicksight:describeAccountCustomPermission",
        "quicksight:describeAccountSettings",
        "quicksight:describeAccountSubscription",
        "quicksight:describeAnalysis",
        "quicksight:describeAnalysisPermissions",
        "quicksight:describeCustomPermissions",
        "quicksight:describeDashboard",
        "quicksight:describeDashboardPermissions",
        "quicksight:describeDataSet",
        "quicksight:describeDataSetPermissions",
        "quicksight:describeDataSetRefreshProperties",
        "quicksight:describeDataSource",
        "quicksight:describeDataSourcePermissions",
```

```
        "quicksight:describeFolder",
        "quicksight:describeFolderPermissions",
        "quicksight:describeFolderResolvedPermissions",
        "quicksight:describeGroup",
        "quicksight:describeGroupMembership",
        "quicksight:describeIAMPolicyAssignment",
        "quicksight:describeIngestion",
        "quicksight:describeIpRestriction",
        "quicksight:describeNamespace",
        "quicksight:describeRefreshSchedule",
        "quicksight:describeRoleCustomPermission",
        "quicksight:describeTemplate",
        "quicksight:describeTemplateAlias",
        "quicksight:describeTemplatePermissions",
        "quicksight:describeTheme",
        "quicksight:describeThemeAlias",
        "quicksight:describeThemePermissions",
        "quicksight:describeTopic",
        "quicksight:describeTopicPermissions",
        "quicksight:describeTopicRefresh",
        "quicksight:describeTopicRefreshSchedule",
        "quicksight:describeUser",
        "quicksight:describeVPCConnection",
        "quicksight:listAnalyses",
        "quicksight:listCustomPermissions",
        "quicksight:listDashboards",
        "quicksight:listDashboardVersions",
        "quicksight:listDataSets",
        "quicksight:listDataSources",
        "quicksight:listFolderMembers",
        "quicksight:listFolders",
        "quicksight:listGroupMemberships",
        "quicksight:listGroups",
        "quicksight:listIAMPolicyAssignments",
        "quicksight:listIAMPolicyAssignmentsForUser",
        "quicksight:listIngestions",
        "quicksight:listNamespaces",
        "quicksight:listRefreshSchedules",
        "quicksight:listTemplateAliases",
        "quicksight:listTemplates",
        "quicksight:listTemplateVersions",
        "quicksight:listThemeAliases",
        "quicksight:listThemes",
        "quicksight:listThemeVersions",
```

```
        "quicksight:listTopicRefreshSchedules",
        "quicksight:listTopics",
        "quicksight:listUserGroups",
        "quicksight:listUsers",
        "quicksight:listVPCConnections",
        "quicksight:searchAnalyses",
        "quicksight:searchDashboards",
        "quicksight:searchDataSets",
        "quicksight:searchDataSources",
        "quicksight:searchFolders",
        "quicksight:searchGroups",
        "ram:getPermission",
        "ram:getResourceShareAssociations",
        "ram:getResourceShareInvitations",
        "ram:getResourceShares",
        "ram:listPendingInvitationResources",
        "ram:listPrincipals",
        "ram:listResources",
        "ram:listResourceSharePermissions",
        "rbin:getRule",
        "rbin:listRules",
        "rds:describeAccountAttributes",
        "rds:describeBlueGreenDeployments",
        "rds:describeCertificates",
        "rds:describeDBClusterAutomatedBackups",
        "rds:describeDBClusterBacktracks",
        "rds:describeDBClusterEndpoints",
        "rds:describeDBClusterParameterGroups",
        "rds:describeDBClusterParameters",
        "rds:describeDBClusters",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusterSnapshotAttributes",
        "rds:describeDBEngineVersions",
        "rds:describeDBInstanceAutomatedBackups",
        "rds:describeDBInstances",
        "rds:describeDBLogFiles",
        "rds:describeDBMajorEngineVersions",
        "rds:describeDBParameterGroups",
        "rds:describeDBParameters",
        "rds:describeDBProxies",
        "rds:describeDBProxyEndpoints",
        "rds:describeDBProxyTargetGroups",
        "rds:describeDBProxyTargets",
        "rds:describeDBRecommendations",
```

```
        "rds:describeDBSecurityGroups",
        "rds:describeDBShardGroups",
        "rds:describeDBSnapshotAttributes",
        "rds:describeDBSnapshots",
        "rds:describeDBSnapshotTenantDatabases",
        "rds:describeDBSubnetGroups",
        "rds:describeEngineDefaultClusterParameters",
        "rds:describeEngineDefaultParameters",
        "rds:describeEventCategories",
        "rds:describeEvents",
        "rds:describeEventSubscriptions",
        "rds:describeExportTasks",
        "rds:describeGlobalClusters",
        "rds:describeIntegrations",
        "rds:describeOptionGroupOptions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describePendingMaintenanceActions",
        "rds:describeReservedDBInstances",
        "rds:describeReservedDBInstancesOfferings",
        "rds:describeSourceRegions",
        "rds:describeTenantDatabases",
        "rds:describeValidDBInstanceModifications",
        "rds:listTagsForResource",
        "redshift-data:describeStatement",
        "redshift-data:listStatements",
        "redshift-serverless:getCustomDomainAssociation",
        "redshift-serverless:getEndpointAccess",
        "redshift-serverless:getNamespace",
        "redshift-serverless:getRecoveryPoint",
        "redshift-serverless:getReservation",
        "redshift-serverless:getReservationOffering",
        "redshift-serverless:getResourcePolicy",
        "redshift-serverless:getScheduledAction",
        "redshift-serverless:getSnapshot",
        "redshift-serverless:getTableRestoreStatus",
        "redshift-serverless:getTrack",
        "redshift-serverless:getUsageLimit",
        "redshift-serverless:getWorkgroup",
        "redshift-serverless:listCustomDomainAssociations",
        "redshift-serverless:listEndpointAccess",
        "redshift-serverless:listManagedWorkgroups",
        "redshift-serverless:listNamespaces",
        "redshift-serverless:listRecoveryPoints",
```

```
        "redshift-serverless:listReservationOfferings",
        "redshift-serverless:listReservations",
        "redshift-serverless:listScheduledActions",
        "redshift-serverless:listSnapshotCopyConfigurations",
        "redshift-serverless:listSnapshots",
        "redshift-serverless:listTableRestoreStatus",
        "redshift-serverless:listUsageLimits",
        "redshift-serverless:listWorkgroups",
        "redshift:describeClusterDbRevisions",
        "redshift:describeClusterParameterGroups",
        "redshift:describeClusterParameters",
        "redshift:describeClusters",
        "redshift:describeClusterSecurityGroups",
        "redshift:describeClusterSnapshots",
        "redshift:describeClusterSubnetGroups",
        "redshift:describeClusterTracks",
        "redshift:describeClusterVersions",
        "redshift:describeCustomDomainAssociations",
        "redshift:describeDataShares",
        "redshift:describeDataSharesForConsumer",
        "redshift:describeDataSharesForProducer",
        "redshift:describeDefaultClusterParameters",
        "redshift:describeEndpointAccess",
        "redshift:describeEndpointAuthorization",
        "redshift:describeEventCategories",
        "redshift:describeEvents",
        "redshift:describeEventSubscriptions",
        "redshift:describeHsmClientCertificates",
        "redshift:describeHsmConfigurations",
        "redshift:describeInboundIntegrations",
        "redshift:describeLoggingStatus",
        "redshift:describeNodeConfigurationOptions",
        "redshift:describeOrderableClusterOptions",
        "redshift:describeRedshiftIdcApplications",
        "redshift:describeReservedNodeOfferings",
        "redshift:describeReservedNodes",
        "redshift:describeResize",
        "redshift:describeSnapshotCopyGrants",
        "redshift:describeSnapshotSchedules",
        "redshift:describeStorage",
        "redshift:describeTableRestoreStatus",
        "redshift:describeTags",
        "redshift:describeUsageLimits",
        "rekognition:listCollections",
```

```
        "rekognition:listFaces",
        "resiliencehub:describeApp",
        "resiliencehub:describeAppAssessment",
        "resiliencehub:describeAppVersion",
        "resiliencehub:describeAppVersionAppComponent",
        "resiliencehub:describeAppVersionResource",
        "resiliencehub:describeAppVersionResourcesResolutionStatus",
        "resiliencehub:describeAppVersionTemplate",
        "resiliencehub:describeDraftAppVersionResourcesImportStatus",
        "resiliencehub:describeResiliencyPolicy",
        "resiliencehub:describeResourceGroupingRecommendationTask",
        "resiliencehub:listAlarmRecommendations",
        "resiliencehub:listAppAssessmentComplianceDrifts",
        "resiliencehub:listAppAssessmentResourceDrifts",
        "resiliencehub:listAppAssessments",
        "resiliencehub:listAppComponentCompliances",
        "resiliencehub:listAppComponentRecommendations",
        "resiliencehub:listAppInputSources",
        "resiliencehub:listApps",
        "resiliencehub:listAppVersionAppComponents",
        "resiliencehub:listAppVersionResourceMappings",
        "resiliencehub:listAppVersionResources",
        "resiliencehub:listAppVersions",
        "resiliencehub:listRecommendationTemplates",
        "resiliencehub:listResiliencyPolicies",
        "resiliencehub:listResourceGroupingRecommendations",
        "resiliencehub:listSopRecommendations",
        "resiliencehub:listSuggestedResiliencyPolicies",
        "resiliencehub:listTestRecommendations",
        "resiliencehub:listUnsupportedAppVersionResources",
        "resource-explorer-2:getAccountLevelServiceConfiguration",
        "resource-explorer-2:getIndex",
        "resource-explorer-2:getView",
        "resource-explorer-2:listIndexes",
        "resource-explorer-2:listViews",
        "resource-explorer-2:search",
        "resource-groups:getGroup",
        "resource-groups:getGroupQuery",
        "resource-groups:getTags",
        "resource-groups:listGroupResources",
        "resource-groups:listGroups",
        "resource-groups:searchResources",
        "robomaker:batchDescribeSimulationJob",
        "robomaker:describeDeploymentJob",
```

```
        "robomaker:describeFleet",
        "robomaker:describeRobot",
        "robomaker:describeRobotApplication",
        "robomaker:describeSimulationApplication",
        "robomaker:describeSimulationJob",
        "robomaker:listDeploymentJobs",
        "robomaker:listFleets",
        "robomaker:listRobotApplications",
        "robomaker:listRobots",
        "robomaker:listSimulationApplications",
        "robomaker:listSimulationJobs",
        "rolesanywhere:getProfile",
        "rolesanywhere:getTrustAnchor",
        "rolesanywhere:listProfiles",
        "rolesanywhere:listTrustAnchors",
        "route53-recovery-cluster:getRoutingControlState",
        "route53-recovery-cluster:listRoutingControls",
        "route53-recovery-control-config:describeCluster",
        "route53-recovery-control-config:describeControlPanel",
        "route53-recovery-control-config:describeRoutingControl",
        "route53-recovery-control-config:describeSafetyRule",
        "route53-recovery-control-config:getResourcePolicy",
        "route53-recovery-control-config:listAssociatedRoute53HealthChecks",
        "route53-recovery-control-config:listClusters",
        "route53-recovery-control-config:listControlPanels",
        "route53-recovery-control-config:listRoutingControls",
        "route53-recovery-control-config:listSafetyRules",
        "route53-recovery-readiness:getArchitectureRecommendations",
        "route53-recovery-readiness:getCell",
        "route53-recovery-readiness:getCellReadinessSummary",
        "route53-recovery-readiness:getReadinessCheck",
        "route53-recovery-readiness:getReadinessCheckResourceStatus",
        "route53-recovery-readiness:getReadinessCheckStatus",
        "route53-recovery-readiness:getRecoveryGroup",
        "route53-recovery-readiness:getRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:listCells",
        "route53-recovery-readiness:listReadinessChecks",
        "route53-recovery-readiness:listCrossAccountAuthorizations",
        "route53-recovery-readiness:listRecoveryGroups",
        "route53-recovery-readiness:listResourceSets",
        "route53-recovery-readiness:listRules",
        "route53:getAccountLimit",
        "route53:getChange",
        "route53:getCheckerIpRanges",
```

```
            "route53:getDNSSEC",
            "route53:getGeoLocation",
            "route53:getHealthCheck",
            "route53:getHealthCheckCount",
            "route53:getHealthCheckLastFailureReason",
            "route53:getHealthCheckStatus",
            "route53:getHostedZone",
            "route53:getHostedZoneCount",
            "route53:getHostedZoneLimit",
            "route53:getQueryLoggingConfig",
            "route53:getReusableDelegationSet",
            "route53:getTrafficPolicy",
            "route53:getTrafficPolicyInstance",
            "route53:getTrafficPolicyInstanceCount",
            "route53:listCidrBlocks",
            "route53:listCidrCollections",
            "route53:listCidrLocations",
            "route53:listGeoLocations",
            "route53:listHealthChecks",
            "route53:listHostedZones",
            "route53:listHostedZonesByName",
            "route53:listHostedZonesByVpc",
            "route53:listQueryLoggingConfigs",
            "route53:listResourceRecordSets",
            "route53:listReusableDelegationSets",
            "route53:listTrafficPolicies",
            "route53:listTrafficPolicyInstances",
            "route53:listTrafficPolicyInstancesByHostedZone",
            "route53:listTrafficPolicyInstancesByPolicy",
            "route53:listTrafficPolicyVersions",
            "route53:listVPCAssociationAuthorizations",
            "route53domains:checkDomainAvailability",
            "route53domains:getContactReachabilityStatus",
            "route53domains:getDomainDetail",
            "route53domains:getOperationDetail",
            "route53domains:listDomains",
            "route53domains:listOperations",
            "route53domains:listPrices",
            "route53domains:listTagsForDomain",
            "route53domains:viewBilling",
            "route53profiles:getProfile",
            "route53profiles:getProfileAssociation",
            "route53profiles:getProfileResourceAssociation",
            "route53profiles:listProfileAssociations",
```

```
        "route53profiles:listProfileResourceAssociations",
        "route53profiles:listProfiles",
        "route53profiles:listTagsForResource",
        "route53resolver:getFirewallConfig",
        "route53resolver:getFirewallDomainList",
        "route53resolver:getFirewallRuleGroup",
        "route53resolver:getFirewallRuleGroupAssociation",
        "route53resolver:getFirewallRuleGroupPolicy",
        "route53resolver:getOutpostResolver",
        "route53resolver:getResolverConfig",
        "route53resolver:getResolverDnssecConfig",
        "route53resolver:getResolverEndpoint",
        "route53resolver:getResolverQueryLogConfig",
        "route53resolver:getResolverQueryLogConfigAssociation",
        "route53resolver:getResolverQueryLogConfigPolicy",
        "route53resolver:getResolverRule",
        "route53resolver:getResolverRuleAssociation",
        "route53resolver:getResolverRulePolicy",
        "route53resolver:listFirewallConfigs",
        "route53resolver:listFirewallDomainLists",
        "route53resolver:listFirewallDomains",
        "route53resolver:listFirewallRuleGroupAssociations",
        "route53resolver:listFirewallRuleGroups",
        "route53resolver:listFirewallRules",
        "route53resolver:listOutpostResolvers",
        "route53resolver:listResolverConfigs",
        "route53resolver:listResolverDnssecConfigs",
        "route53resolver:listResolverEndpointIpAddresses",
        "route53resolver:listResolverEndpoints",
        "route53resolver:listResolverQueryLogConfigAssociations",
        "route53resolver:listResolverQueryLogConfigs",
        "route53resolver:listResolverRuleAssociations",
        "route53resolver:listResolverRules",
        "route53resolver:listTagsForResource",
        "route53globalresolver:getAccessSource",
        "route53globalresolver:getAccessToken",
        "route53globalresolver:getDNSView",
        "route53globalresolver:getFirewallDomainList",
        "route53globalresolver:getFirewallRule",
        "route53globalresolver:getGlobalResolver",
        "route53globalresolver:getHostedZoneAssociation",
        "route53globalresolver:getManagedFirewallDomainList",
        "route53globalresolver:listAccessSources",
        "route53globalresolver:listAccessTokens",
```

```
        "route53globalresolver:listDNSViews",
        "route53globalresolver:listFirewallDomainLists",
        "route53globalresolver:listFirewallDomains",
        "route53globalresolver:listFirewallRules",
        "route53globalresolver:listGlobalResolvers",
        "route53globalresolver:listHostedZoneAssociations",
        "route53globalresolver:listManagedFirewallDomainLists",
        "rum:batchGetRumMetricDefinitions",
        "rum:getAppMonitor",
        "rum:listAppMonitors",
        "rum:listRumMetricsDestinations",
        "s3-outposts:getLifecycleConfiguration",
        "s3-outposts:getAccessPoint",
        "s3-outposts:getAccessPointPolicy",
        "s3-outposts:getBucketPolicy",
        "s3-outposts:getBucketVersioning",
        "s3-outposts:getReplicationConfiguration",
        "s3-outposts:listAccessPoints",
        "s3-outposts:listEndpoints",
        "s3-outposts:listOutpostsWithS3",
        "s3-outposts:listRegionalBuckets",
        "s3-outposts:listSharedEndpoints",
        "s3:describeJob",
        "s3:describeMultiRegionAccessPointOperation",
        "s3:getAccelerateConfiguration",
        "s3:getAccessGrant",
        "s3:getAccessGrantsInstance",
        "s3:getAccessGrantsInstanceResourcePolicy",
        "s3:getAccessGrantsLocation",
        "s3:getAccessPoint",
        "s3:getAccessPointConfigurationForObjectLambda",
        "s3:getAccessPointForObjectLambda",
        "s3:getAccessPointPolicy",
        "s3:getAccessPointPolicyForObjectLambda",
        "s3:getAccessPointPolicyStatus",
        "s3:getAccessPointPolicyStatusForObjectLambda",
        "s3:getAccountPublicAccessBlock",
        "s3:getAnalyticsConfiguration",
        "s3:getBucketAcl",
        "s3:getBucketCORS",
        "s3:getBucketLocation",
        "s3:getBucketLogging",
        "s3:getBucketNotification",
        "s3:getBucketObjectLockConfiguration",
```

```
        "s3:getBucketOwnershipControls",
        "s3:getBucketPolicy",
        "s3:getBucketPolicyStatus",
        "s3:getBucketPublicAccessBlock",
        "s3:getBucketRequestPayment",
        "s3:getBucketVersioning",
        "s3:getBucketWebsite",
        "s3:getEncryptionConfiguration",
        "s3:getIntelligentTieringConfiguration",
        "s3:getInventoryConfiguration",
        "s3:getLifecycleConfiguration",
        "s3:getMetricsConfiguration",
        "s3:getMultiRegionAccessPoint",
        "s3:getMultiRegionAccessPointPolicy",
        "s3:getMultiRegionAccessPointPolicyStatus",
        "s3:getMultiRegionAccessPointRoutes",
        "s3:getObjectAcl",
        "s3:getObjectLegalHold",
        "s3:getObjectRetention",
        "s3:getReplicationConfiguration",
        "s3:getStorageLensConfiguration",
        "s3:listAccessGrants",
        "s3:listAccessGrantsInstances",
        "s3:listAccessGrantsLocations",
        "s3:listAccessPoints",
        "s3:listAccessPointsForObjectLambda",
        "s3:listAllMyBuckets",
        "s3:listBucket",
        "s3:listBucketMultipartUploads",
        "s3:listBucketVersions",
        "s3:listJobs",
        "s3:listMultipartUploadParts",
        "s3:listMultiRegionAccessPoints",
        "s3:listStorageLensConfigurations",
        "s3express:getBucketPolicy",
        "s3express:listAllMyDirectoryBuckets",
        "s3files:getAccessPoint",
        "s3files:getFileSystem",
        "s3files:getFileSystemPolicy",
        "s3files:getMountTarget",
        "s3files:getSynchronizationConfiguration",
        "s3files:listAccessPoints",
        "s3files:listFileSystems",
        "s3files:listMountTargets",
```

```
        "s3files:listTagsForResource",
        "s3tables:getNamespace",
        "s3tables:getTable",
        "s3tables:getTableBucket",
        "s3tables:getTableBucketEncryption",
        "s3tables:getTableBucketMaintenanceConfiguration",
        "s3tables:getTableBucketMetricsConfiguration",
        "s3tables:getTableBucketPolicy",
        "s3tables:getTableBucketReplication",
        "s3tables:getTableBucketStorageClass",
        "s3tables:getTableEncryption",
        "s3tables:getTableMaintenanceConfiguration",
        "s3tables:getTableMaintenanceJobStatus",
        "s3tables:getTableMetadataLocation",
        "s3tables:getTablePolicy",
        "s3tables:getTableRecordExpirationConfiguration",
        "s3tables:getTableRecordExpirationJobStatus",
        "s3tables:getTableReplication",
        "s3tables:getTableReplicationStatus",
        "s3tables:getTableStorageClass",
        "s3tables:listNamespaces",
        "s3tables:listTableBuckets",
        "s3tables:listTables",
        "s3vectors:getIndex",
        "s3vectors:getVectorBucket",
        "s3vectors:getVectorBucketPolicy",
        "s3vectors:listIndexes",
        "s3vectors:listVectorBuckets",
        "sagemaker:describeAction",
        "sagemaker:describeAlgorithm",
        "sagemaker:describeApp",
        "sagemaker:describeAppImageConfig",
        "sagemaker:describeArtifact",
        "sagemaker:describeAutoMLJob",
        "sagemaker:describeAutoMLJobV2",
        "sagemaker:describeCluster",
        "sagemaker:describeClusterNode",
        "sagemaker:describeClusterEvent",
        "sagemaker:describeClusterSchedulerConfig",
        "sagemaker:describeCodeRepository",
        "sagemaker:describeCompilationJob",
        "sagemaker:describeComputeQuota",
        "sagemaker:describeContext",
        "sagemaker:describeDataQualityJobDefinition",
```

```
        "sagemaker:describeDevice",
        "sagemaker:describeDeviceFleet",
        "sagemaker:describeDomain",
        "sagemaker:describeEdgeDeploymentPlan",
        "sagemaker:describeEdgePackagingJob",
        "sagemaker:describeEndpoint",
        "sagemaker:describeEndpointConfig",
        "sagemaker:describeExperiment",
        "sagemaker:describeFeatureGroup",
        "sagemaker:describeFeatureMetadata",
        "sagemaker:describeFlowDefinition",
        "sagemaker:describeHub",
        "sagemaker:describeHubContent",
        "sagemaker:describeHumanTaskUi",
        "sagemaker:describeHyperParameterTuningJob",
        "sagemaker:describeImage",
        "sagemaker:describeImageVersion",
        "sagemaker:describeInferenceComponent",
        "sagemaker:describeInferenceExperiment",
        "sagemaker:describeInferenceRecommendationsJob",
        "sagemaker:describeLabelingJob",
        "sagemaker:describeLineageGroup",
        "sagemaker:describeMlflowApp",
        "sagemaker:describeMlflowTrackingServer",
        "sagemaker:describeModel",
        "sagemaker:describeModelBiasJobDefinition",
        "sagemaker:describeModelCard",
        "sagemaker:describeModelCardExportJob",
        "sagemaker:describeModelExplainabilityJobDefinition",
        "sagemaker:describeModelPackage",
        "sagemaker:describeModelPackageGroup",
        "sagemaker:describeModelQualityJobDefinition",
        "sagemaker:describeMonitoringSchedule",
        "sagemaker:describeNotebookInstance",
        "sagemaker:describeNotebookInstanceLifecycleConfig",
        "sagemaker:describeOptimizationJob",
        "sagemaker:describePipeline",
        "sagemaker:describePipelineDefinitionForExecution",
        "sagemaker:describePipelineExecution",
        "sagemaker:describePartnerApp",
        "sagemaker:describeProcessingJob",
        "sagemaker:describeProject",
        "sagemaker:describeReservedCapacity",
        "sagemaker:describeSpace",
```

```
        "sagemaker:describeStudioLifecycleConfig",
        "sagemaker:describeSubscribedWorkteam",
        "sagemaker:describeTrainingJob",
        "sagemaker:describeTrainingPlan",
        "sagemaker:describeTransformJob",
        "sagemaker:describeTrial",
        "sagemaker:describeTrialComponent",
        "sagemaker:describeUserProfile",
        "sagemaker:describeWorkforce",
        "sagemaker:describeWorkteam",
        "sagemaker:getDeviceFleetReport",
        "sagemaker:getModelPackageGroupPolicy",
        "sagemaker:getLineageGroupPolicy",
        "sagemaker:getSagemakerServicecatalogPortfolioStatus",
        "sagemaker:listActions",
        "sagemaker:listAlgorithms",
        "sagemaker:listAliases",
        "sagemaker:listAppImageConfigs",
        "sagemaker:listApps",
        "sagemaker:listArtifacts",
        "sagemaker:listAssociations",
        "sagemaker:listAutoMLJobs",
        "sagemaker:listCandidatesForAutoMLJob",
        "sagemaker:listClusterNodes",
        "sagemaker:listClusters",
        "sagemaker:listClusterEvents",
        "sagemaker:listClusterSchedulerConfigs",
        "sagemaker:listCodeRepositories",
        "sagemaker:listCompilationJobs",
        "sagemaker:listComputeQuotas",
        "sagemaker:listContexts",
        "sagemaker:listDataQualityJobDefinitions",
        "sagemaker:listDeviceFleets",
        "sagemaker:listDevices",
        "sagemaker:listDomains",
        "sagemaker:listEdgeDeploymentPlans",
        "sagemaker:listEdgePackagingJobs",
        "sagemaker:listEndpointConfigs",
        "sagemaker:listEndpoints",
        "sagemaker:listExperiments",
        "sagemaker:listFeatureGroups",
        "sagemaker:listFlowDefinitions",
        "sagemaker:listHubContents",
        "sagemaker:listHubContentVersions",
```

```
        "sagemaker:listHubs",
        "sagemaker:listHumanTaskUis",
        "sagemaker:listHyperParameterTuningJobs",
        "sagemaker:listImages",
        "sagemaker:listImageVersions",
        "sagemaker:listInferenceComponents",
        "sagemaker:listInferenceExperiments",
        "sagemaker:listInferenceRecommendationsJobs",
        "sagemaker:listInferenceRecommendationsJobSteps",
        "sagemaker:listLabelingJobs",
        "sagemaker:listLabelingJobsForWorkteam",
        "sagemaker:listLineageGroups",
        "sagemaker:listMlflowApps",
        "sagemaker:listMlflowTrackingServers",
        "sagemaker:listModelBiasJobDefinitions",
        "sagemaker:listModelCardExportJobs",
        "sagemaker:listModelCards",
        "sagemaker:listModelCardVersions",
        "sagemaker:listModelExplainabilityJobDefinitions",
        "sagemaker:listModelMetadata",
        "sagemaker:listModelPackageGroups",
        "sagemaker:listModelPackages",
        "sagemaker:listModelQualityJobDefinitions",
        "sagemaker:listModels",
        "sagemaker:listMonitoringAlertHistory",
        "sagemaker:listMonitoringAlerts",
        "sagemaker:listMonitoringExecutions",
        "sagemaker:listMonitoringSchedules",
        "sagemaker:listNotebookInstanceLifecycleConfigs",
        "sagemaker:listNotebookInstances",
        "sagemaker:listOptimizationJobs",
        "sagemaker:listPartnerApps",
        "sagemaker:listPipelineExecutions",
        "sagemaker:listPipelineExecutionSteps",
        "sagemaker:listPipelineParametersForExecution",
        "sagemaker:listPipelines",
        "sagemaker:listPipelineVersions",
        "sagemaker:listProcessingJobs",
        "sagemaker:listProjects",
        "sagemaker:listResourceCatalogs",
        "sagemaker:listSpaces",
        "sagemaker:listStageDevices",
        "sagemaker:listStudioLifecycleConfigs",
        "sagemaker:listSubscribedWorkteams",
```

```
        "sagemaker:listTags",
        "sagemaker:listTrainingJobs",
        "sagemaker:listTrainingJobsForHyperParameterTuningJob",
        "sagemaker:listTrainingPlans",
        "sagemaker:listTransformJobs",
        "sagemaker:listTrialComponents",
        "sagemaker:listTrials",
        "sagemaker:listUserProfiles",
        "sagemaker:listUltraServersByReservedCapacity",
        "sagemaker:listWorkforces",
        "sagemaker:listWorkteams",
        "sagemaker:search",
        "savingsplans:describeSavingsPlanRates",
        "savingsplans:describeSavingsPlans",
        "savingsplans:describeSavingsPlansOfferingRates",
        "savingsplans:describeSavingsPlansOfferings",
        "scheduler:getSchedule",
        "scheduler:getScheduleGroup",
        "scheduler:listScheduleGroups",
        "scheduler:listSchedules",
        "schemas:describeCodeBinding",
        "schemas:describeDiscoverer",
        "schemas:describeRegistry",
        "schemas:describeSchema",
        "schemas:getCodeBindingSource",
        "schemas:getDiscoveredSchema",
        "schemas:getResourcePolicy",
        "schemas:listDiscoverers",
        "schemas:listRegistries",
        "schemas:listSchemas",
        "schemas:listSchemaVersions",
        "sdb:domainMetadata",
        "sdb:listDomains",
        "secretsmanager:describeSecret",
        "secretsmanager:getResourcePolicy",
        "secretsmanager:listSecrets",
        "secretsmanager:listSecretVersionIds",
        "security-ir:batchGetMemberAccountDetails",
        "security-ir:getMembership",
        "security-ir:listCases",
        "security-ir:listMemberships",
        "securityhub:batchGetAutomationRules",
        "securityhub:batchGetConfigurationPolicyAssociations",
        "securityhub:describeHub",
```

```
        "securityhub:describeOrganizationConfiguration",
        "securityhub:describeProductsV2",
        "securityhub:describeSecurityHubV2",
        "securityhub:getConfigurationPolicy",
        "securityhub:getConfigurationPolicyAssociation",
        "securityhub:getEnabledStandards",
        "securityhub:getFindingAggregator",
        "securityhub:getFindingHistory",
        "securityhub:getFindings",
        "securityhub:getInsightResults",
        "securityhub:getInsights",
        "securityhub:getMasterAccount",
        "securityhub:getMembers",
        "securityhub:getAggregatorV2",
        "securityhub:getAutomationRuleV2",
        "securityhub:getConnectorV2",
        "securityhub:getResourcesV2",
        "securityhub:listAutomationRules",
        "securityhub:listConfigurationPolicies",
        "securityhub:listConfigurationPolicyAssociations",
        "securityhub:listEnabledProductsForImport",
        "securityhub:listFindingAggregators",
        "securityhub:listInvitations",
        "securityhub:listMembers",
        "securityhub:listAggregatorsV2",
        "securityhub:listAutomationRulesV2",
        "securityhub:listConnectorsV2",
        "securitylake:getDataLakeExceptionSubscription",
        "securitylake:getDataLakeOrganizationConfiguration",
        "securitylake:getDataLakeSources",
        "securitylake:getSubscriber",
        "securitylake:listDataLakeExceptions",
        "securitylake:listDataLakes",
        "securitylake:listLogSources",
        "securitylake:listSubscribers",
        "serverlessrepo:getApplication",
        "serverlessrepo:getApplicationPolicy",
        "serverlessrepo:getCloudFormationTemplate",
        "serverlessrepo:listApplicationDependencies",
        "serverlessrepo:listApplications",
        "serverlessrepo:listApplicationVersions",
        "servicecatalog:describeConstraint",
        "servicecatalog:describePortfolio",
        "servicecatalog:describeProduct",
```

```
        "servicecatalog:describeProductAsAdmin",
        "servicecatalog:describeProductView",
        "servicecatalog:describeProvisioningArtifact",
        "servicecatalog:describeProvisioningParameters",
        "servicecatalog:describeRecord",
        "servicecatalog:listAcceptedPortfolioShares",
        "servicecatalog:listConstraintsForPortfolio",
        "servicecatalog:listLaunchPaths",
        "servicecatalog:listPortfolioAccess",
        "servicecatalog:listPortfolios",
        "servicecatalog:listPortfoliosForProduct",
        "servicecatalog:listPrincipalsForPortfolio",
        "servicecatalog:listProvisioningArtifacts",
        "servicecatalog:listRecordHistory",
        "servicecatalog:scanProvisionedProducts",
        "servicecatalog:searchProducts",
        "servicequotas:getAssociationForServiceQuotaTemplate",
        "servicequotas:getAWSDefaultServiceQuota",
        "servicequotas:getRequestedServiceQuotaChange",
        "servicequotas:getServiceQuota",
        "servicequotas:getServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:listAWSDefaultServiceQuotas",
        "servicequotas:listRequestedServiceQuotaChangeHistory",
        "servicequotas:listRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:listServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:listServiceQuotas",
        "servicequotas:listServices",
        "ses:batchGetMetricData",
        "ses:describeActiveReceiptRuleSet",
        "ses:describeConfigurationSet",
        "ses:describeReceiptRule",
        "ses:describeReceiptRuleSet",
        "ses:getAccount",
        "ses:getAccountSendingEnabled",
        "ses:getAddonInstance",
        "ses:getAddonSubscription",
        "ses:getArchive",
        "ses:getArchiveExport",
        "ses:getArchiveSearch",
        "ses:getArchiveSearchResults",
        "ses:getBlacklistReports",
        "ses:getConfigurationSet",
        "ses:getConfigurationSetEventDestinations",
        "ses:getContactList",
```

```
        "ses:getDedicatedIp",
        "ses:getDedicatedIpPool",
        "ses:getDedicatedIps",
        "ses:getDeliverabilityDashboardOptions",
        "ses:getDeliverabilityTestReport",
        "ses:getDomainDeliverabilityCampaign",
        "ses:getDomainStatisticsReport",
        "ses:getEmailIdentity",
        "ses:getIdentityDkimAttributes",
        "ses:getIdentityMailFromDomainAttributes",
        "ses:getIdentityNotificationAttributes",
        "ses:getIdentityPolicies",
        "ses:getIdentityVerificationAttributes",
        "ses:getImportJob",
        "ses:getIngressPoint",
        "ses:getMessageInsights",
        "ses:getRelay",
        "ses:getRuleSet",
        "ses:getTrafficPolicy",
        "ses:getSendQuota",
        "ses:getSendStatistics",
        "ses:listConfigurationSets",
        "ses:listAddonInstances",
        "ses:listAddonSubscriptions",
        "ses:listArchiveExports",
        "ses:listArchives",
        "ses:listArchiveSearches",
        "ses:listContactLists",
        "ses:listContacts",
        "ses:listCustomVerificationEmailTemplates",
        "ses:listDedicatedIpPools",
        "ses:listDeliverabilityTestReports",
        "ses:listDomainDeliverabilityCampaigns",
        "ses:listEmailIdentities",
        "ses:listEmailTemplates",
        "ses:listIdentities",
        "ses:listIdentityPolicies",
        "ses:listImportJobs",
        "ses:listIngressPoints",
        "ses:listReceiptFilters",
        "ses:listReceiptRuleSets",
        "ses:listRelays",
        "ses:listRuleSets",
        "ses:listRecommendations",
```

```
        "ses:listTagsForResource",
        "ses:listTemplates",
        "ses:listTrafficPolicies",
        "ses:listVerifiedEmailAddresses",
        "shield:describeAttack",
        "shield:describeAttackStatistics",
        "shield:describeDRTAccess",
        "shield:describeProtection",
        "shield:describeProtectionGroup",
        "shield:describeSubscription",
        "shield:getSubscriptionState",
        "shield:listAttacks",
        "shield:listProtectionGroups",
        "shield:listProtections",
        "signer:describeSigningJob",
        "signer:getRevocationStatus",
        "signer:getSigningPlatform",
        "signer:getSigningProfile",
        "signer:listProfilePermissions",
        "signer:listSigningJobs",
        "signer:listSigningPlatforms",
        "signer:listSigningProfiles",
        "sms-voice:describeAccountAttributes",
        "sms-voice:describeSpendLimits",
        "sms-voice:describeVerifiedDestinationNumbers",
        "sms-voice:getConfigurationSetEventDestinations",
        "sms:getConnectors",
        "sms:getReplicationJobs",
        "sms:getReplicationRuns",
        "sms:getServers",
        "snowball:describeAddress",
        "snowball:describeAddresses",
        "snowball:describeJob",
        "snowball:getSnowballUsage",
        "snowball:listJobs",
        "snowball:listServiceVersions",
        "sns:checkIfPhoneNumberIsOptedOut",
        "sns:getDataProtectionPolicy",
        "sns:getEndpointAttributes",
        "sns:getPlatformApplicationAttributes",
        "sns:getSMSAttributes",
        "sns:getSMSSandboxAccountStatus",
        "sns:getSubscriptionAttributes",
        "sns:getTopicAttributes",
```

```
        "sns:listEndpointsByPlatformApplication",
        "sns:listOriginationNumbers",
        "sns:listPhoneNumbersOptedOut",
        "sns:listPlatformApplications",
        "sns:listSMSSandboxPhoneNumbers",
        "sns:listSubscriptions",
        "sns:listSubscriptionsByTopic",
        "sns:listTopics",
        "sqs:getQueueAttributes",
        "sqs:getQueueUrl",
        "sqs:listDeadLetterSourceQueues",
        "sqs:listMessageMoveTasks",
        "sqs:listQueues",
        "ssm-contacts:describeEngagement",
        "ssm-contacts:describePage",
        "ssm-contacts:getContact",
        "ssm-contacts:getContactChannel",
        "ssm-contacts:getContactPolicy",
        "ssm-contacts:getRotation",
        "ssm-contacts:getRotationOverride",
        "ssm-contacts:listContactChannels",
        "ssm-contacts:listContacts",
        "ssm-contacts:listEngagements",
        "ssm-contacts:listPageReceipts",
        "ssm-contacts:listPageResolutions",
        "ssm-contacts:listPagesByContact",
        "ssm-contacts:listPagesByEngagement",
        "ssm-contacts:listPreviewRotationShifts",
        "ssm-contacts:listRotationOverrides",
        "ssm-contacts:listRotations",
        "ssm-contacts:listRotationShifts",
        "ssm-incidents:batchGetIncidentFindings",
        "ssm-incidents:getIncidentRecord",
        "ssm-incidents:getReplicationSet",
        "ssm-incidents:getResourcePolicies",
        "ssm-incidents:getResponsePlan",
        "ssm-incidents:getTimelineEvent",
        "ssm-incidents:listIncidentFindings",
        "ssm-incidents:listIncidentRecords",
        "ssm-incidents:listRelatedItems",
        "ssm-incidents:listReplicationSets",
        "ssm-incidents:listResponsePlans",
        "ssm-incidents:listTimelineEvents",
        "ssm-quicksetup:getConfiguration",
```

```
        "ssm-quicksetup:getConfigurationManager",
        "ssm-quicksetup:getServiceSettings",
        "ssm-quicksetup:listConfigurationManagers",
        "ssm-quicksetup:listConfigurations",
        "ssm-quicksetup:listQuickSetupTypes",
        "ssm-sap:getApplication",
        "ssm-sap:getComponent",
        "ssm-sap:getConfigurationCheckOperation",
        "ssm-sap:getDatabase",
        "ssm-sap:getOperation",
        "ssm-sap:getResourcePermission",
        "ssm-sap:listApplications",
        "ssm-sap:listComponents",
        "ssm-sap:listConfigurationCheckDefinitions",
        "ssm-sap:listConfigurationCheckOperations",
        "ssm-sap:listDatabases",
        "ssm-sap:listOperations",
        "ssm-sap:listSubCheckResults",
        "ssm-sap:listSubCheckRuleResults",
        "ssm:describeActivations",
        "ssm:describeAssociation",
        "ssm:describeAssociationExecutions",
        "ssm:describeAssociationExecutionTargets",
        "ssm:describeAutomationExecutions",
        "ssm:describeAutomationStepExecutions",
        "ssm:describeAvailablePatches",
        "ssm:describeDocument",
        "ssm:describeDocumentPermission",
        "ssm:describeEffectiveInstanceAssociations",
        "ssm:describeEffectivePatchesForPatchBaseline",
        "ssm:describeInstanceAssociationsStatus",
        "ssm:describeInstanceInformation",
        "ssm:describeInstancePatches",
        "ssm:describeInstancePatchStates",
        "ssm:describeInstancePatchStatesForPatchGroup",
        "ssm:describeInstanceProperties",
        "ssm:describeInventoryDeletions",
        "ssm:describeMaintenanceWindowExecutions",
        "ssm:describeMaintenanceWindowExecutionTaskInvocations",
        "ssm:describeMaintenanceWindowExecutionTasks",
        "ssm:describeMaintenanceWindows",
        "ssm:describeMaintenanceWindowSchedule",
        "ssm:describeMaintenanceWindowsForTarget",
        "ssm:describeMaintenanceWindowTargets",
```

```
        "ssm:describeMaintenanceWindowTasks",
        "ssm:describeOpsItems",
        "ssm:describeParameters",
        "ssm:describePatchBaselines",
        "ssm:describePatchGroups",
        "ssm:describePatchGroupState",
        "ssm:describePatchProperties",
        "ssm:describeSessions",
        "ssm:getAutomationExecution",
        "ssm:getCalendarState",
        "ssm:getCommandInvocation",
        "ssm:getConnectionStatus",
        "ssm:getDefaultPatchBaseline",
        "ssm:getDeployablePatchSnapshotForInstance",
        "ssm:getInventorySchema",
        "ssm:getMaintenanceWindow",
        "ssm:getMaintenanceWindowExecution",
        "ssm:getMaintenanceWindowExecutionTask",
        "ssm:getMaintenanceWindowExecutionTaskInvocation",
        "ssm:getMaintenanceWindowTask",
        "ssm:getOpsItem",
        "ssm:getOpsMetadata",
        "ssm:getOpsSummary",
        "ssm:getPatchBaseline",
        "ssm:getPatchBaselineForPatchGroup",
        "ssm:getResourcePolicies",
        "ssm:getServiceSetting",
        "ssm:listAssociations",
        "ssm:listAssociationVersions",
        "ssm:listCommandInvocations",
        "ssm:listCommands",
        "ssm:listComplianceItems",
        "ssm:listComplianceSummaries",
        "ssm:listDocumentMetadataHistory",
        "ssm:listDocuments",
        "ssm:listDocumentVersions",
        "ssm:listNodes",
        "ssm:listNodesSummary",
        "ssm:listOpsItemEvents",
        "ssm:listOpsItemRelatedItems",
        "ssm:listOpsMetadata",
        "ssm:listResourceComplianceSummaries",
        "ssm:listResourceDataSync",
        "ssm:listTagsForResource",
```

```
        "sso:describeApplication",
        "sso:describeApplicationAssignment",
        "sso:describeApplicationProvider",
        "sso:describeAccountAssignmentCreationStatus",
        "sso:describeAccountAssignmentDeletionStatus",
        "sso:describeInstance",
        "sso:describeInstanceAccessControlAttributeConfiguration",
        "sso:describePermissionSet",
        "sso:describePermissionSetProvisioningStatus",
        "sso:describeTrustedTokenIssuer",
        "sso:getApplicationAccessScope",
        "sso:getApplicationAssignmentConfiguration",
        "sso:getApplicationAuthenticationMethod",
        "sso:getApplicationGrant",
        "sso:getApplicationInstance",
        "sso:getApplicationTemplate",
        "sso:getInlinePolicyForPermissionSet",
        "sso:getManagedApplicationInstance",
        "sso:getPermissionsBoundaryForPermissionSet",
        "sso:getSharedSsoConfiguration",
        "sso:listApplicationAccessScopes",
        "sso:listApplicationAssignments",
        "sso:listApplicationAuthenticationMethods",
        "sso:listApplicationGrants",
        "sso:listApplicationInstances",
        "sso:listApplicationProviders",
        "sso:listApplications",
        "sso:listApplicationTemplates",
        "sso:listAccountAssignmentCreationStatus",
        "sso:listAccountAssignmentDeletionStatus",
        "sso:listAccountAssignments",
        "sso:listAccountAssignmentsForPrincipal",
        "sso:listAccountsForProvisionedPermissionSet",
        "sso:listApplicationAssignmentsForPrincipal",
        "sso:listCustomerManagedPolicyReferencesInPermissionSet",
        "sso:listDirectoryAssociations",
        "sso:listInstances",
        "sso:listManagedPoliciesInPermissionSet",
        "sso:listPermissionSetProvisioningStatus",
        "sso:listPermissionSets",
        "sso:listPermissionSetsProvisionedToAccount",
        "sso:listProfileAssociations",
        "sso:listTrustedTokenIssuers",
        "states:describeActivity",
```

```
        "states:describeExecution",
        "states:describeMapRun",
        "states:describeStateMachine",
        "states:describeStateMachineAlias",
        "states:describeStateMachineForExecution",
        "states:getExecutionHistory",
        "states:listActivities",
        "states:listExecutions",
        "states:listMapRuns",
        "states:listStateMachineAliases",
        "states:listStateMachines",
        "states:listStateMachineVersions",
        "storagegateway:describeBandwidthRateLimit",
        "storagegateway:describeCache",
        "storagegateway:describeCachediSCSIVolumes",
        "storagegateway:describeFileSystemAssociations",
        "storagegateway:describeGatewayInformation",
        "storagegateway:describeMaintenanceStartTime",
        "storagegateway:describeNFSFileShares",
        "storagegateway:describeSMBFileShares",
        "storagegateway:describeSMBSettings",
        "storagegateway:describeSnapshotSchedule",
        "storagegateway:describeStorediSCSIVolumes",
        "storagegateway:describeTapeArchives",
        "storagegateway:describeTapeRecoveryPoints",
        "storagegateway:describeTapes",
        "storagegateway:describeUploadBuffer",
        "storagegateway:describeVTLDevices",
        "storagegateway:describeWorkingStorage",
        "storagegateway:listAutomaticTapeCreationPolicies",
        "storagegateway:listFileShares",
        "storagegateway:listFileSystemAssociations",
        "storagegateway:listGateways",
        "storagegateway:listLocalDisks",
        "storagegateway:listTagsForResource",
        "storagegateway:listTapes",
        "storagegateway:listVolumeInitiators",
        "storagegateway:listVolumeRecoveryPoints",
        "storagegateway:listVolumes",
        "sts:getCallerIdentity",
        "swf:countClosedWorkflowExecutions",
        "swf:countOpenWorkflowExecutions",
        "swf:countPendingActivityTasks",
        "swf:countPendingDecisionTasks",
```

```
        "swf:describeActivityType",
        "swf:describeDomain",
        "swf:describeWorkflowExecution",
        "swf:describeWorkflowType",
        "swf:getWorkflowExecutionHistory",
        "swf:listActivityTypes",
        "swf:listClosedWorkflowExecutions",
        "swf:listDomains",
        "swf:listOpenWorkflowExecutions",
        "swf:listWorkflowTypes",
        "sustainability:getEstimatedCarbonEmissions",
        "sustainability:getEstimatedCarbonEmissionsDimensionValues",
        "sustainability:getEstimatedWaterAllocation",
        "sustainability:getEstimatedWaterAllocationDimensionValues",
        "synthetics:describeCanaries",
        "synthetics:describeCanariesLastRun",
        "synthetics:describeRuntimeVersions",
        "synthetics:getCanary",
        "synthetics:getCanaryRuns",
        "synthetics:getGroup",
        "synthetics:listAssociatedGroups",
        "synthetics:listGroupResources",
        "synthetics:listGroups",
        "tax:getTaxInheritance",
        "tax:getTaxRegistration",
        "thinclient:getDevice",
        "thinclient:getEnvironment",
        "thinclient:getSoftwareSet",
        "thinclient:listDevices",
        "thinclient:listEnvironments",
        "thinclient:listSoftwareSets",
        "timestream:describeAccountSettings",
        "timestream:describeBatchLoadTask",
        "timestream:describeDatabase",
        "timestream:describeEndpoints",
        "timestream:describeScheduledQuery",
        "timestream:describeTable",
        "timestream:listBatchLoadTasks",
        "timestream:listDatabases",
        "timestream:listScheduledQueries",
        "timestream:listTables",
        "tiros:createQuery",
        "tiros:getQueryAnswer",
        "tiros:getQueryExplanation",
```

```
        "tnb:getSolFunctionInstance",
        "tnb:getSolFunctionPackage",
        "tnb:getSolNetworkInstance",
        "tnb:getSolNetworkOperation",
        "tnb:getSolNetworkPackage",
        "tnb:listSolFunctionInstances",
        "tnb:listSolFunctionPackages",
        "tnb:listSolNetworkInstances",
        "tnb:listSolNetworkOperations",
        "tnb:listSolNetworkPackages",
        "transcribe:describeLanguageModel",
        "transcribe:getCallAnalyticsCategory",
        "transcribe:getCallAnalyticsJob",
        "transcribe:getMedicalTranscriptionJob",
        "transcribe:getMedicalVocabulary",
        "transcribe:getTranscriptionJob",
        "transcribe:getVocabulary",
        "transcribe:getVocabularyFilter",
        "transcribe:listCallAnalyticsCategories",
        "transcribe:listCallAnalyticsJobs",
        "transcribe:listLanguageModels",
        "transcribe:listMedicalTranscriptionJobs",
        "transcribe:listMedicalVocabularies",
        "transcribe:listTranscriptionJobs",
        "transcribe:listVocabularies",
        "transcribe:listVocabularyFilters",
        "transfer:describeAccess",
        "transfer:describeAgreement",
        "transfer:describeConnector",
        "transfer:describeExecution",
        "transfer:describeProfile",
        "transfer:describeServer",
        "transfer:describeUser",
        "transfer:describeWebApp",
        "transfer:describeWebAppCustomization",
        "transfer:describeWorkflow",
        "transfer:listAccesses",
        "transfer:listAgreements",
        "transfer:listConnectors",
        "transfer:listExecutions",
        "transfer:listHostKeys",
        "transfer:listProfiles",
        "transfer:listServers",
        "transfer:listTagsForResource",
```

```
        "transfer:listUsers",
        "transfer:listWebApps",
        "transfer:listWorkflows",
        "transfer:sendWorkflowStepState",
        "trustedadvisor:getOrganizationRecommendation",
        "trustedadvisor:getRecommendation",
        "trustedadvisor:listChecks",
        "trustedadvisor:listOrganizationRecommendationAccounts",
        "trustedadvisor:listOrganizationRecommendationResources",
        "trustedadvisor:listOrganizationRecommendations",
        "trustedadvisor:listRecommendationResources",
        "trustedadvisor:listRecommendations",
        "verifiedpermissions:getIdentitySource",
        "verifiedpermissions:getPolicy",
        "verifiedpermissions:getPolicyStore",
        "verifiedpermissions:getPolicyTemplate",
        "verifiedpermissions:getSchema",
        "verifiedpermissions:listIdentitySources",
        "verifiedpermissions:listPolicies",
        "verifiedpermissions:listPolicyStores",
        "verifiedpermissions:listPolicyTemplates",
        "vpc-lattice:getAccessLogSubscription",
        "vpc-lattice:getAuthPolicy",
        "vpc-lattice:getDomainVerification",
        "vpc-lattice:getListener",
        "vpc-lattice:getResourceConfiguration",
        "vpc-lattice:getResourceGateway",
        "vpc-lattice:getResourcePolicy",
        "vpc-lattice:getRule",
        "vpc-lattice:getService",
        "vpc-lattice:getServiceNetwork",
        "vpc-lattice:getServiceNetworkResourceAssociation",
        "vpc-lattice:getServiceNetworkServiceAssociation",
        "vpc-lattice:getServiceNetworkVpcAssociation",
        "vpc-lattice:getTargetGroup",
        "vpc-lattice:listAccessLogSubscriptions",
        "vpc-lattice:listDomainVerifications",
        "vpc-lattice:listListeners",
        "vpc-lattice:listResourceConfigurations",
        "vpc-lattice:listResourceEndpointAssociations",
        "vpc-lattice:listResourceGateways",
        "vpc-lattice:listRules",
        "vpc-lattice:listServiceNetworks",
        "vpc-lattice:listServiceNetworkResourceAssociations",
```

```
        "vpc-lattice:listServiceNetworkServiceAssociations",
        "vpc-lattice:listServiceNetworkVpcAssociations",
        "vpc-lattice:listServiceNetworkVpcEndpointAssociations",
        "vpc-lattice:listServices",
        "vpc-lattice:listTargetGroups",
        "vpc-lattice:listTargets",
        "waf-regional:getByteMatchSet",
        "waf-regional:getChangeTokenStatus",
        "waf-regional:getGeoMatchSet",
        "waf-regional:getIPSet",
        "waf-regional:getLoggingConfiguration",
        "waf-regional:getRateBasedRule",
        "waf-regional:getRegexMatchSet",
        "waf-regional:getRegexPatternSet",
        "waf-regional:getRule",
        "waf-regional:getRuleGroup",
        "waf-regional:getSqlInjectionMatchSet",
        "waf-regional:getWebACL",
        "waf-regional:getWebACLForResource",
        "waf-regional:listActivatedRulesInRuleGroup",
        "waf-regional:listByteMatchSets",
        "waf-regional:listGeoMatchSets",
        "waf-regional:listIPSets",
        "waf-regional:listLoggingConfigurations",
        "waf-regional:listRateBasedRules",
        "waf-regional:listRegexMatchSets",
        "waf-regional:listRegexPatternSets",
        "waf-regional:listResourcesForWebACL",
        "waf-regional:listRuleGroups",
        "waf-regional:listRules",
        "waf-regional:listSqlInjectionMatchSets",
        "waf-regional:listWebACLs",
        "waf:getByteMatchSet",
        "waf:getChangeTokenStatus",
        "waf:getGeoMatchSet",
        "waf:getIPSet",
        "waf:getLoggingConfiguration",
        "waf:getRateBasedRule",
        "waf:getRegexMatchSet",
        "waf:getRegexPatternSet",
        "waf:getRule",
        "waf:getRuleGroup",
        "waf:getSampledRequests",
        "waf:getSizeConstraintSet",
```

```
        "waf:getSqlInjectionMatchSet",
        "waf:getWebACL",
        "waf:getXssMatchSet",
        "waf:listActivatedRulesInRuleGroup",
        "waf:listByteMatchSets",
        "waf:listGeoMatchSets",
        "waf:listIPSets",
        "waf:listLoggingConfigurations",
        "waf:listRateBasedRules",
        "waf:listRegexMatchSets",
        "waf:listRegexPatternSets",
        "waf:listRuleGroups",
        "waf:listRules",
        "waf:listSizeConstraintSets",
        "waf:listSqlInjectionMatchSets",
        "waf:listWebACLs",
        "waf:listXssMatchSets",
        "wafv2:checkCapacity",
        "wafv2:describeManagedRuleGroup",
        "wafv2:getIPSet",
        "wafv2:getLoggingConfiguration",
        "wafv2:getPermissionPolicy",
        "wafv2:getRateBasedStatementManagedKeys",
        "wafv2:getRegexPatternSet",
        "wafv2:getRuleGroup",
        "wafv2:getSampledRequests",
        "wafv2:getWebACL",
        "wafv2:getWebACLForResource",
        "wafv2:listAvailableManagedRuleGroups",
        "wafv2:listIPSets",
        "wafv2:listLoggingConfigurations",
        "wafv2:listRegexPatternSets",
        "wafv2:listResourcesForWebACL",
        "wafv2:listRuleGroups",
        "wafv2:listTagsForResource",
        "wafv2:listWebACLs",
        "workdocs:checkAlias",
        "workdocs:describeAvailableDirectories",
        "workdocs:describeInstances",
        "workmail:describeGroup",
        "workmail:describeOrganization",
        "workmail:describeResource",
        "workmail:describeUser",
        "workmail:listAliases",
```

```
        "workmail:listGroupMembers",
        "workmail:listGroups",
        "workmail:listMailboxPermissions",
        "workmail:listOrganizations",
        "workmail:listResourceDelegates",
        "workmail:listResources",
        "workmail:listUsers",
        "workspaces-web:getBrowserSettings",
        "workspaces-web:getIdentityProvider",
        "workspaces-web:getNetworkSettings",
        "workspaces-web:getPortal",
        "workspaces-web:getPortalServiceProviderMetadata",
        "workspaces-web:getTrustStoreCertificate",
        "workspaces-web:getUserSettings",
        "workspaces-web:listBrowserSettings",
        "workspaces-web:listIdentityProviders",
        "workspaces-web:listNetworkSettings",
        "workspaces-web:listPortals",
        "workspaces-web:listTagsForResource",
        "workspaces-web:listTrustStoreCertificates",
        "workspaces-web:listTrustStores",
        "workspaces-web:listUserSettings",
        "workspaces:describeAccount",
        "workspaces:describeAccountModifications",
        "workspaces:describeApplicationAssociations",
        "workspaces:describeCustomWorkspaceImageImport",
        "workspaces:describeIpGroups",
        "workspaces:describeTags",
        "workspaces:describeWorkspaceAssociations",
        "workspaces:describeWorkspaceBundles",
        "workspaces:describeWorkspaceDirectories",
        "workspaces:describeWorkspaceImages",
        "workspaces:describeWorkspaces",
        "workspaces:describeWorkspaceSnapshots",
        "workspaces:describeWorkspacesConnectionStatus",
        "workspaces:describeWorkspacesPools",
        "workspaces:describeWorkspacesPoolSessions",
        "xray:getEncryptionConfig",
        "xray:getGroup",
        "xray:getGroups",
        "xray:getInsightImpactGraph",
        "xray:getSamplingRules",
        "xray:getSamplingStatisticSummaries",
        "xray:getSamplingTargets",
```

```
        "xray:getServiceGraph",
        "xray:getTimeSeriesServiceStatistics",
        "xray:getTraceGraph",
        "xray:listResourcePolicies"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSystemsManagerAccountDiscoveryServicePolicy

Descrição: Concede permissão ao AWS Systems Manager (SSM) para descobrir Conta da AWS informações.

`AWSSystemsManagerAccountDiscoveryServicePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 24 de outubro de 2019, 17:21 UTC
- Hora da edição: 17 de outubro de 2022, 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSystemsManagerChangeManagementServicePolicy

Descrição: Fornece acesso aos AWS recursos gerenciados ou usados pela estrutura de gerenciamento de mudanças do AWS Systems Manager.

`AWSSystemsManagerChangeManagementServicePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 07 de dezembro de 2020, 22:21 UTC
- Horário editado: 23 de outubro de 2025, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation",
```

```
        "ssm:CreateOpsItem",
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:GetAutomationExecution",
        "ssm:GetCalendarState",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:IsMemberInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetGroup",
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSystemsManagerEnableConfigRecordingExecutionPolicy

Descrição: Fornece permissões para que a Configuração Rápida do AWS Systems Manager ative e configure a gravação da configuração do AWS Config.

`AWSSystemsManagerEnableConfigRecordingExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSystemsManagerEnableConfigRecordingExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de junho de 2024, 9:40 UTC
- Hora da edição: 26 de junho de 2024, 9:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerEnableConfigRecordingExecutionPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3BucketCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-quick-setup-config-recording-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SNSTopicsListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DefaultSNSTopicCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:ConfigRecording-Default-Topic"
```

```
    },
    {
      "Sid" : "ConfigureAndStartConfigurationRecorderPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeDeliveryChannels",
        "config:PutConfigurationRecorder",
        "config:PutDeliveryChannel",
        "config:StartConfigurationRecorder"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetAndPassConfigSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
        "arn:aws:iam::*:role/AWSServiceRoleForConfig"
      ]
    },
    {
      "Sid" : "CreateConfigSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSystemsManagerEnableExplorerExecutionPolicy

Descrição: Essa política concede permissões administrativas para habilitar o Explorer, um recurso do AWS Systems Manager. Isso inclui permissões para atualizar as configurações de serviços relacionados do Systems Manager e criar um perfil vinculado ao serviço para o Systems Manager.

`AWSSystemsManagerEnableExplorerExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSystemsManagerEnableExplorerExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de junho de 2024, 9:42 UTC
- Hora da edição: 26 de junho de 2024, 9:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
```

```
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSystemsManagerForSAPFullAccess

Descrição: Fornece acesso total ao serviço AWS Systems Manager for SAP

`AWSSystemsManagerForSAPFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSystemsManagerForSAPFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de novembro de 2022, 2:11 UTC
- Hora da edição: 10 julho de 2024, 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsSsmForSapPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    },
    {
      "Sid" : "AwsSsmForSapServiceRoleCreationPermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm-sap.amazonaws.com/
AWSServiceRoleForAWSSSMForSAP"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm-sap.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2StartStopPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
```

```
          "ec2:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSystemsManagerForSAPReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao serviço AWS Systems Manager for SAP

`AWSSystemsManagerForSAPReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSystemsManagerForSAPReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 17 de novembro de 2022, 2:11 UTC
- Hora da edição: 17 de novembro de 2022, 2:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSystemsManagerJustInTimeAccessServicePolicy

Descrição: Fornece acesso aos AWS recursos gerenciados ou usados pela estrutura de acesso just-in time do AWS Systems Manager.

`AWSSystemsManagerJustInTimeAccessServicePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 21 de abril de 2025, 20:07 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerJustInTimeAccessServicePolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOpsItemReplication",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "Replica"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AllowOpsItemReplicationTagging",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "Replica"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAutomationExecutionTagging",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOpsItemManagement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowRetrieveDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : [
            "ManualApprovalPolicy",
            "AutoApprovalPolicy"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDescriptions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeOpsItems",
        "ssm:DescribeSessions",
        "ssm:ListDocuments"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "AllowListTagsForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*"
      ]
    },
    {
      "Sid" : "AllowListSSMGUIConnections",
      "Effect" : "Allow",
      "Action" : [
        "ssm-guiconnect:ListConnections"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowIdentityStoreActions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetUserId"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSODirectoryActions",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:IsMemberInGroup"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "AllowSSOInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribingEC2Tags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowPublishingCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/SSM/JustInTimeAccess"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSystemsManagerJustInTimeAccessTokenPolicy

Descrição: A política gerenciada AWSSystemsManagerJustInTimeAccessTokenPolicy permite que o Systems Manager gere tokens de acesso usados para acesso aos nós just-in-time.

`AWSSystemsManagerJustInTimeAccessTokenPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSystemsManagerJustInTimeAccessTokenPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 17 de abril de 2025, 21:07 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenPolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Sid" : "TerminateAndResumeSessionAndOpenDataChannel",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:TerminateSession",
        "ssm:ResumeSession",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Sid" : "GuiConnect",
      "Effect" : "Allow",
      "Action" : [
        "ssm-guiconnect:CancelConnection",
        "ssm-guiconnect:GetConnection",
        "ssm-guiconnect:StartConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SessionManagerKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RdpKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm-guiconnect.*.amazonaws.com"
        },
```

```
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "RdpStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWS-StartPortForwardingSession"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetup",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListDirectoryAssociations*",
        "identitystore:DescribeUser",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetupSendCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWSSSO-CreateSSOUser"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSystemsManagerJustInTimeAccessTokenSessionPolicy

Descrição: A política gerenciada AWSSystemsManagerJustInTimeAccessTokenSessionPolicy permite que o Systems Manager aplique permissões com escopo reduzido a uma sessão de acesso ao nó just-in-time depois de iniciada.

`AWSSystemsManagerJustInTimeAccessTokenSessionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSystemsManagerJustInTimeAccessTokenSessionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 17 de abril de 2025, 20:52 UTC
- Horário editado: 12 de fevereiro de 2026, 18:03 UTC

- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenSessionPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Sid" : "GuiConnect",
      "Effect" : "Allow",
      "Action" : [
        "ssm-guiconnect:CancelConnection",
        "ssm-guiconnect:GetConnection",
        "ssm-guiconnect:StartConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SessionManagerKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
```

```
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RdpKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm-guiconnect.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "RdpStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-StartPortForwardingSession"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetup",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sso:ListDirectoryAssociations*",
        "identitystore:DescribeUser",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetupSendCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSSSO-CreateSSOUser"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy

Descrição: essa política permite que o Systems Manager compartilhe uma política de acesso ou negação de acesso a nós just-in-time da conta do administrador delegado para as contas de membros e replique a política em várias regiões.

`AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 21 de abril de 2025, 20:52 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QuickSetupPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-quicksetup:GetConfigurationManager",
        "cloudformation:ListStackSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QuickSetupOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "ssm-quicksetup.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "QuickSetupSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm-quicksetup.amazonaws.com/
AWSServiceRoleForSSMQuickSetup"
      ]
    },
    {
      "Sid" : "OrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMDocumentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
```

```
        "ssm:DescribeDocument",
        "ssm:ListTagsForResource",
        "ssm:PutResourcePolicy",
        "ssm:DeleteResourcePolicy",
        "ssm:GetResourcePolicies"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : "AutoApprovalPolicy"
        }
      }
    },
    {
      "Sid" : "SSMDocumentCreateReplicaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : "AutoApprovalPolicy",
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "SSMDocumentUpdateReplicaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateDocument",
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:UpdateDocumentMetadata",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
```

```
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : "AutoApprovalPolicy",
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "ssm:Document"
        },
        "ArnLikeIfExists" : {
          "ram:ResourceArn" : "arn:aws:ssm:*:*:document/SSM-
JustInTimeAccessDenyAccessOrgPolicy"
        }
      }
    },
    {
      "Sid" : "RAMTaggingPermissions",
      "Effect" : "Allow",
```

```
      "Action" : "ram:TagResource",
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RAMModificationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:ResourceShareName" : "SSMJustInTimeNodeAccessManagedResourceShare",
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "ssm:Document"
        },
        "ArnLikeIfExists" : {
          "ram:ResourceArn" : "arn:aws:ssm:*:*:document/SSM-
JustInTimeAccessDenyAccessOrgPolicy"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSystemsManagerNotificationsServicePolicy

Descrição: Permissões necessárias para coletar informações sobre um usuário para Just-In-Time-Node-Access notificações.

`AWSSystemsManagerNotificationsServicePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 17 de abril de 2025, 20:52 UTC
- Horário editado: 17 de abril de 2025, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerNotificationsServicePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "AllowIdentityStoreActions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroupMemberships",
        "identitystore:DescribeUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSOActions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSODirectoryActions",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUser",
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowIamActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "*"
      ]
    }
```

```
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSSystemsManagerOpsDataSyncServiceRolePolicy

Descrição: função do IAM para o SSM Explorer para gerenciar operações OpsData relacionadas

`AWSSystemsManagerOpsDataSyncServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 26 de abril de 2021, 20:42 UTC
- Hora da edição: 28 de junho de 2023, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ExplorerSecurityHubOpsItem" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "securityhub:GetFindings",
        "securityhub:BatchUpdateFindings"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "securityhub:ASFFSyntaxPath/Workflow.Status" : "SUPPRESSED"
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Confidence" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Criticality" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
```

```
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Note.Text" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Note.UpdatedBy" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/RelatedFindings" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Types" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/UserDefinedFields.key" : false
        }
```

```
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/UserDefinedFields.value" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/VerificationState" : false
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSThinkboxAssetServerPolicy

Descrição: Essa política concede ao AWS Portal Asset Server as permissões necessárias para a operação normal.

`AWSThinkboxAssetServerPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSThinkboxAssetServerPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de maio de 2020, 19:18 UTC
- Hora da edição: 27 de maio de 2020, 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
```

```
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSThinkboxAWSPortalAdminPolicy

Descrição: Esta política concede ao software Deadline da AWS Thinkbox acesso total a vários AWS serviços, conforme necessário para a administração AWS do Portal. Isso inclui acesso para criar tags arbitrárias em vários tipos de recursos do EC2.

`AWSThinkboxAWSPortalAdminPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSThinkboxAWSPortalAdminPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de maio de 2020, 19:41 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxAWSPortal1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAddresses",
        "ec2:DescribeFleets",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNatGateways",
        "ec2:DescribeTags",
        "ec2:DescribeKeyPairs",
        "ec2:DescribePlacementGroups",
```

```
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRegions",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:GetConsoleOutput",
        "ec2:ImportKeyPair",
        "ec2:ReleaseAddress",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:DisassociateAddress",
        "ec2:DeleteFleets",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteVpc",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DeleteNatGateway",
        "ec2:DetachInternetGateway",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyFleet",
        "ec2:ModifySpotFleetRequest",
        "ec2:ModifyVpcAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal2",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:key-pair/*",
```

```
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal3",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/AWSPortal*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal4",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ReverseForwarder"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal5",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : false
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal6",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:PlacementGroup" : "arn:aws:ec2:*:*:placement-group/
*DeadlinePlacementGroup*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ArnLike" : {
          "ec2:PlacementGroup" : "arn:aws:ec2:*:*:placement-group/
*DeadlinePlacementGroup*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal10",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal11",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AWSPortal*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal12",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicyVersions"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/AWSPortal*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal13",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal14",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal15",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal16",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketVersioning",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:PutBucketLogging",
        "s3:PutBucketTagging",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3::*:awsportal*",
        "arn:aws:s3::*:stack*",
        "arn:aws:s3::*:aws-portal-cache*",
        "arn:aws:s3::*:logs-for-aws-portal-cache*",
        "arn:aws:s3::*:logs-for-stack*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal17",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3::*:logs-for-aws-portal-cache*"
```

```
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal18",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3::*:logs-for-stack*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal19",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal20",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal21",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
```

```
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/stack*/*",
        "arn:aws:cloudformation:*:*:stack/Deadline*/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal22",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:EstimateTemplateCost",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal23",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DeleteRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/thinkbox*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal24",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal25",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
```

```
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal26",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : [
            "rcs-tls-pw*"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal27",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSThinkboxAWSPortalGatewayPolicy

Descrição: Essa política concede à máquina do AWS Portal Gateway as permissões necessárias para a operação normal.

`AWSThinkboxAWSPortalGatewayPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSThinkboxAWSPortalGatewayPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de maio de 2020, 19:05 UTC
- Hora da edição: 30 de junho de 2020, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "dynamodb:Scan",
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::stack*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*/gateway_certs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw-stack*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSThinkboxAWSPortalWorkerPolicy

Descrição: Essa política concede aos Deadline Workers in AWS Portal as permissões necessárias para a operação normal.

`AWSThinkboxAWSPortalWorkerPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSThinkboxAWSPortalWorkerPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de maio de 2020, 19:15 UTC
- Hora da edição: 07 de dezembro de 2020, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineRole" : "DeadlineRenderNode"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*/gateway_certs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWS*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSThinkboxDeadlineResourceTrackerAccessPolicy

Descrição: Concede as permissões necessárias para a operação do Deadline Resource Tracker da AWS Thinkbox. Isso inclui acesso total a algumas ações do EC2, incluindo DeleteFleets e. CancelSpotFleetRequests

`AWSThinkboxDeadlineResourceTrackerAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSThinkboxDeadlineResourceTrackerAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 27 de maio de 2020, 19:25 UTC
- Hora da edição: 27 de maio de 2020, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb:DeleteItem",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:PutItem",
        "dynamodb:Scan",
        "dynamodb:UpdateItem",
        "dynamodb:UpdateTable"
```

```
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelSpotFleetRequests",
        "ec2:DeleteFleets",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeFleets",
        "ec2:DescribeInstances",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/DeadlineTrackedAWSResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutEvents"
      ],
      "Resource" : [
        "arn:aws:events:*:*:event-bus/default"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:ReceiveMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeStateMessageQueue*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSThinkboxDeadlineResourceTrackerAdminPolicy

Descrição: Concede as permissões necessárias para criar, destruir e administrar o Deadline Resource Tracker da AWS Thinkbox.

`AWSThinkboxDeadlineResourceTrackerAdminPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSThinkboxDeadlineResourceTrackerAdminPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de maio de 2020, 19:29 UTC
- Horário editado: 16 de julho de 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker1",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker2",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker3",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
```

```
        "arn:aws:cloudformation:*:*:stack/DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker4",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable",
        "dynamodb:ListTagsOfResource",
        "dynamodb:TagResource",
        "dynamodb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker5",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb:Scan"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker6",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DeadlineResourceTracker*"
      ]
```

```
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker7",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker8",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker9",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker10",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTrackerAccess*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker11",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/dynamodb.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_DynamoDBTable"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker12",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker13",
      "Effect" : "Allow",
      "Action" : [
```

```
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "lambda:FunctionArn" : [
            "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker14",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ],
      "Condition" : {
        "StringLike" : {
          "lambda:Principal" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker15",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:DeleteFunctionConcurrency",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "lambda:PutFunctionConcurrency",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
```

```
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker16",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/deadline_aws_resource_tracker*.zip",
        "arn:aws:s3:::*/DeadlineAWSResourceTrackerTemplate*.yaml"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker17",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:TagQueue",
        "sqs:UntagQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*",
        "arn:aws:sqs:*:*:DeadlineResourceTracker*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

Descrição: Concede as permissões necessárias para o plug-in de eventos Deadline Spot da AWS Thinkbox. Isso inclui permissão para solicitar, modificar e cancelar uma frota spot, bem como PassRole permissão limitada.

`AWSThinkboxDeadlineSpotEventPluginAdminPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSThinkboxDeadlineSpotEventPluginAdminPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de maio de 2020, 19:38 UTC
- Hora da edição: 27 de maio de 2020, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelSpotFleetRequests",
        "ec2:DescribeSpotFleetInstances",
```

```
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:RequestSpotFleet"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

Descrição: Conceda as permissões necessárias para uma instância do EC2 executando o software AWS Thinkbox Deadline Spot Event Plugin Worker.

`AWSThinkboxDeadlineSpotEventPluginWorkerPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSThinkboxDeadlineSpotEventPluginWorkerPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de maio de 2020, 19:35 UTC
- Hora da edição: 07 de dezembro de 2020, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineTrackedAWSResource" : "SpotEventPlugin"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineResourceTracker" : "SpotEventPlugin"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueUrl",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransferConsoleFullAccess

Descrição: Fornece acesso total à AWS transferência por meio do Console de gerenciamento da AWS

`AWSTransferConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTransferConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de dezembro de 2020, 19:33 UTC
- Hora da edição: 14 de dezembro de 2020, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "transfer.amazonaws.com"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "health:DescribeEventAggregates",
        "iam:GetPolicyVersion",
        "iam:ListPolicies",
        "iam:ListRoles",
        "route53:ListHostedZones",
        "s3:ListAllMyBuckets",
        "transfer:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransferFullAccess

Descrição: Fornece acesso total ao Serviço AWS de Transferência.

`AWSTransferFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTransferFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de dezembro de 2020, 19:37 UTC
- Hora da edição: 14 de dezembro de 2020, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "transfer:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "transfer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransferLoggingAccess

Descrição: Permite AWS transferir acesso total para criar fluxos de log e grupos e colocar eventos de log em sua conta

`AWSTransferLoggingAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTransferLoggingAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 14 de janeiro de 2019, 15:32 UTC
- Hora da edição: 14 de janeiro de 2019, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransferReadOnlyAccess

Descrição: Forneça acesso somente para leitura aos serviços AWS de transferência.

`AWSTransferReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTransferReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de agosto de 2020, 17:54 UTC
- Hora da edição: 27 de agosto de 2020, 17:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransferServiceRolePolicy

Descrição: Permite que o Transfer se integre a outros AWS serviços em seu nome

`AWSTransferServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 22 de setembro de 2026, 17:07 UTC
- Horário editado: 22 de setembro de 2026, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTransferServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TransferSecretsManagerBatchAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:BatchGetSecretValue",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TransferSecretsManagerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:transfer!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "transfer",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TransferSecretsManagerDeleteAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:transfer!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "transfer",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        },
        "Bool" : {
          "secretsmanager:ForceDeleteWithoutRecovery" : false
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransformApplicationDeploymentPolicy

Descrição: permite que o serviço AWS Transform implante aplicativos.NET transformados criando e gerenciando AWS recursos. Essa política concede permissões para provisionar infraestrutura, gerenciar recursos de computação e definir configurações de implantação em vários AWS serviços.

`AWSTransformApplicationDeploymentPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTransformApplicationDeploymentPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 28 de agosto de 2025, 06:34 UTC
- Horário editado: 11 de setembro de 2026, 00:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransformApplicationDeploymentPolicy`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSTransform*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
```

```
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAnyValue:StringNotEquals" : {
          "aws:TagKeys" : [
            "Name",
            "CreatedBy",
            "ApplicationName",
            "TransformationType",
            "aws:cloudformation:stack-name",
            "aws:cloudformation:logical-id",
            "aws:cloudformation:stack-id"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:instance-profile/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-App-Instance-Role",
        "arn:aws:iam::*:instance-profile/AWSTransform-Deploy-App-Instance-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-App-Instance-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/ami-amazon-linux-latest*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:ModifyInstanceAttribute"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunRemoteScript"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:AbortMultipartUpload",
        "s3:PutBucketTagging"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-transform-deployment-bucket-*",
        "arn:aws:s3:::aws-transform-deployment-bucket-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedFor" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws-transform" : "*",
```

```
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:ebs:id" : "*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "*"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransformApplicationECSDeploymentPolicy

Descrição: Permite que o AWS Transform implante aplicativos no Amazon Elastic Container Service (ECS) com o Fargate. Ela concede permissões para provisionar, configurar e gerenciar a infraestrutura subjacente necessária para executar aplicações no ECS.

`AWSTransformApplicationECSDeploymentPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTransformApplicationECSDeploymentPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 29 de setembro de 2025, 22:49 UTC

- Horário editado: 11 de setembro de 2026, 00:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransformApplicationECSDeploymentPolicy`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:CreateStack",
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
```

```
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack",
            "UpdateStack"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:CreateCluster",
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:UpdateCluster",
        "ecs:DeleteCluster"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ecs:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:RegisterTaskDefinition",
      "Resource" : "arn:aws:ecs:*:*:task-definition/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:RunTask",
      "Resource" : "arn:aws:ecs:*:*:task-definition/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        },
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:ListTasks",
      "Resource" : "arn:aws:ecs:*:*:container-instance/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        },
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:DescribeTasks",
      "Resource" : "arn:aws:ecs:*:*:task/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Task-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Execution-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com",
            "ecs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Task-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Execution-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:CreateService",
      "Resource" : "arn:aws:ecs:*:*:service/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:DeleteService"
      ],
      "Resource" : "arn:aws:ecs:*:*:service/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ecs:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/AWSTransform*",
        "arn:aws:ecs:*:*:task-definition/AWSTransform*",
```

```
        "arn:aws:ecs:*:*:service/AWSTransform*",
        "arn:aws:ecs:*:*:task/AWSTransform*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:UntagResource",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*:log-stream:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/awstransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
```

```
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Bool" : {
```

```
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ecr.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:ecr:arn" : "*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "GenerateDataKey"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransformCustomExecuteTransformations

Descrição: Fornece acesso para executar transformações no AWS Transform custom.

`AWSTransformCustomExecuteTransformations` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTransformCustomExecuteTransformations` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 05 de dezembro de 2025, 15:34 UTC
- Horário editado: 27 de abril de 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformCustomExecuteTransformations`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomExecuteTransformations",
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:ConverseStream",
        "transform-custom:ExecuteTransformation",
        "transform-custom:GetCampaign",
        "transform-custom:UpdateCampaignRepositoryStatus",
        "transform-custom:UpdateCampaign"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/transform-custom.amazonaws.com/
AWSServiceRoleForAWSTransformCustom"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "transform-custom.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransformCustomFullAccess

Descrição: Fornece acesso total ao AWS Transform custom.

`AWSTransformCustomFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTransformCustomFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 05 de dezembro de 2025, 15:19 UTC
- Horário editado: 07 de abril de 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformCustomFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomAllActions",
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/transform-custom.amazonaws.com/
AWSServiceRoleForAWSTransformCustom"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "transform-custom.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransformCustomManageTransformations

Descrição: Permite o gerenciamento de recursos de transformação e a execução de transformações no AWS Transform custom.

`AWSTransformCustomManageTransformations` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTransformCustomManageTransformations` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 05 de dezembro de 2025, 15:49 UTC
- Horário editado: 27 de abril de 2026, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformCustomManageTransformations`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomManageTransformations",
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:ConverseStream",
        "transform-custom:CreateTransformationPackageUrl",
        "transform-custom:CompleteTransformationPackageUpload",
        "transform-custom:DeleteTransformationPackage",
        "transform-custom:GetTransformationPackageUrl",
        "transform-custom:ListTransformationPackageMetadata",
        "transform-custom:ExecuteTransformation",
        "transform-custom:ListKnowledgeItems",
        "transform-custom:GetKnowledgeItem",
        "transform-custom:DeleteKnowledgeItem",
        "transform-custom:UpdateKnowledgeItemConfiguration",
        "transform-custom:UpdateKnowledgeItemStatus",
        "transform-custom:GetCampaign",
        "transform-custom:UpdateCampaignRepositoryStatus",
        "transform-custom:UpdateCampaign",
        "transform-custom:ListTagsForResource",
        "transform-custom:TagResource",
        "transform-custom:UntagResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/transform-custom.amazonaws.com/
AWSServiceRoleForAWSTransformCustom"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "transform-custom.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransformInfrastructureExecutorAccessBatch

Descrição: concede aos desenvolvedores a função de execução as permissões necessárias para executar a Modernização Contínua de AWS Transformação CLI/agent para ser executada assessments/transformations usando o AWS Batch, incluindo o upload do código-fonte, a recuperação de resultados, o monitoramento do status do trabalho em lote, a leitura de registros e o gerenciamento de cronogramas de transformação.

`AWSTransformInfrastructureExecutorAccessBatch` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTransformInfrastructureExecutorAccessBatch` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 20 de julho de 2026, 20:12 UTC
- Horário editado: 02 de setembro de 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformInfrastructureExecutorAccessBatch`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LambdaInvokeATXFunctions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:GetFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:atx-trigger-job-*",
        "arn:aws:lambda:*:*:function:atx-trigger-batch-jobs-*",
        "arn:aws:lambda:*:*:function:atx-get-job-status-*",
        "arn:aws:lambda:*:*:function:atx-get-batch-status-*",
        "arn:aws:lambda:*:*:function:atx-list-jobs-*",
        "arn:aws:lambda:*:*:function:atx-list-batches-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3UploadSourceCode",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::atx-source-code-*",
        "arn:aws:s3:::atx-source-code-*/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3DownloadResults",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::atx-custom-output-*",
        "arn:aws:s3:::atx-custom-output-*/*",
        "arn:aws:s3:::atx-ct-output-*",
        "arn:aws:s3:::atx-ct-output-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3WriteBatchSidecar",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::atx-custom-output-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSEncryptDecrypt",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : [
            "alias/atx-encryption-key",
            "alias/atx-encryption-key-*"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchReadLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/batch/atx-transform*",
        "arn:aws:logs:*:*:log-group:/aws/batch/job*",
        "arn:aws:logs:*:*:log-group:AtxVpc*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/atx-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchDashboard",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetDashboard",
        "cloudwatch:ListDashboards"
```

```
      ],
      "Resource" : [
        "arn:aws:cloudwatch::*:dashboard/ATX-Transform-CLI-Dashboard",
        "arn:aws:cloudwatch::*:dashboard/ATX-Transform-CLI-Dashboard-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BatchDescribe",
      "Effect" : "Allow",
      "Action" : [
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobs",
        "batch:ListJobs"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CheckInfrastructureStatus",
      "Effect" : "Allow",
      "Action" : "cloudformation:DescribeStacks",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AtxInfrastructureStack/*",
        "arn:aws:cloudformation:*:*:stack/AtxInfrastructureStack-*/*",
        "arn:aws:cloudformation:*:*:stack/atx-*",
        "arn:aws:cloudformation:*:*:stack/atx-*/*",
        "arn:aws:cloudformation:*:*:stack/AtxSecurityAgentStack-*/*",
        "arn:aws:cloudformation:*:*:stack/AtxDispatcherStack/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "SecretsManagerATXSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SchedulerManage",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:DeleteSchedule",
        "scheduler:GetSchedule",
        "scheduler:UpdateSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListSchedules"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule-group/atx-ct",
        "arn:aws:scheduler:*:*:schedule-group/atx-ct-*",
        "arn:aws:scheduler:*:*:schedule/atx-ct/*",
        "arn:aws:scheduler:*:*:schedule/atx-ct-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassSchedulerRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
```

```
        "arn:aws:iam::*:role/AtxSchedulerInvocationRole",
        "arn:aws:iam::*:role/AtxSchedulerInvocationRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "scheduler.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2NetworkDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNatGateways"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMReadRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/ATX*",
        "arn:aws:iam::*:role/Atx*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "TagGetATXStacks",
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CFNListStacksForDetect",
      "Effect" : "Allow",
      "Action" : "cloudformation:ListStacks",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SQSEnqueueToDispatcher",
      "Effect" : "Allow",
      "Action" : "sqs:SendMessage",
      "Resource" : "arn:aws:sqs:*:*:atx-dispatcher-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransformInfrastructureExecutorAccessEC2

Descrição: Concede aos desenvolvedores a função de execução as permissões necessárias para executar o AWS Transform Continuous Modernization CLI/agent para ser executado assessments/transformations usando o EC2, incluindo o upload do código-fonte, a recuperação de resultados, o monitoramento do status do trabalho, a leitura de registros e o gerenciamento de cronogramas de transformação.

`AWSTransformInfrastructureExecutorAccessEC2` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTransformInfrastructureExecutorAccessEC2` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 20 de julho de 2026, 20:12 UTC
- Horário editado: 02 de setembro de 2026, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformInfrastructureExecutorAccessEC2`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "CFNRead",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStackDriftDetectionStatus"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/atx-*/*",
        "arn:aws:cloudformation:*:*:stack/AtxSecurityAgentStack-*/*",
        "arn:aws:cloudformation:*:*:stack/AtxDispatcherStack/*"
      ]
    },
    {
      "Sid" : "CFNValidateTemplate",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Desc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNatGateways",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2PowerState",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/atx-remote-infra" : "true"
        }
      }
    },
    {
      "Sid" : "SSMRead",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeSessions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SSMTgt",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/atx-remote-infra" : "true"
        }
      }
    },
    {
      "Sid" : "SSMDocs",
```

```
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*::document/AWS-RunShellScript"
    },
    {
      "Sid" : "S3Data",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::atx-source-code-*",
        "arn:aws:s3:::atx-source-code-*/*",
        "arn:aws:s3:::atx-ct-output-*",
        "arn:aws:s3:::atx-ct-output-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSEncryptDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : [
            "alias/atx-encryption-key",
            "alias/atx-encryption-key-*"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "SM",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SMList",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SchedLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:DeleteSchedule",
        "scheduler:GetSchedule",
        "scheduler:UpdateSchedule"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule/atx-ct/*",
        "arn:aws:scheduler:*:*:schedule/atx-ct-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "SchedGroupRead",
      "Effect" : "Allow",
      "Action" : "scheduler:GetScheduleGroup",
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule-group/atx-ct",
        "arn:aws:scheduler:*:*:schedule-group/atx-ct-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SchedList",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassEC2InstanceRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/atx-transform-role",
        "arn:aws:iam::*:role/atx-transform-role-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "IAMPassSchedulerRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AtxSchedulerInvocationRole",
        "arn:aws:iam::*:role/AtxSchedulerInvocationRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "scheduler.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMReadRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/atx-*",
        "arn:aws:iam::*:role/Atx*",
        "arn:aws:iam::*:role/ATX*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMReadInstanceProfile",
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/atx-*",
        "arn:aws:iam::*:instance-profile/Atx*",
        "arn:aws:iam::*:instance-profile/ATX*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagGetATXStacks",
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CFNListStacksForDetect",
      "Effect" : "Allow",
      "Action" : "cloudformation:ListStacks",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SQSEnqueueToDispatcher",
      "Effect" : "Allow",
      "Action" : "sqs:SendMessage",
      "Resource" : "arn:aws:sqs:*:*:atx-dispatcher-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransformLandingZoneAgentPolicy

Descrição: Concede permissões ao AWS Transform para configurar zonas de AWS destino, incluindo provisionamento de contas, governança organizacional e configuração da Torre de Controle

`AWSTransformLandingZoneAgentPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTransformLandingZoneAgentPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 06 de agosto de 2026, 15:12 UTC
- Horário editado: 01 de setembro de 2026, 10:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformLandingZoneAgentPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3LandingZoneBucketAndObjectOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetObject",
        "s3:GetObjectAttributes",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:PutBucketPolicy",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::transform-vmware-landing-zone-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnLandingZoneStackCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AtxLz*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnLandingZoneStackUpdate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AtxLz*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnLandingZoneStackOperationsAndChangeSets",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:ListChangeSets"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AtxLz*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ControlTowerAndOrganizationsOperationsReadOnly",
```

```
      "Effect" : "Allow",
      "Action" : [
        "controltower:GetBaselineOperation",
        "controltower:GetControlOperation",
        "controltower:ListBaselines",
        "controltower:ListEnabledBaselines",
        "controltower:ListEnabledControls",
        "controltower:ListLandingZones",
        "organizations:DescribeCreateAccountStatus",
        "organizations:DescribeOrganization",
        "organizations:ListPolicies",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ControlTowerResourceOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "controltower:GetEnabledBaseline",
        "controltower:GetEnabledControl",
        "controltower:GetLandingZone",
        "controltower:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:controltower:*:*:enabledbaseline/*",
        "arn:aws:controltower:*:*:enabledcontrol/*",
        "arn:aws:controltower:*:*:landingzone/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ControlTowerBaselineOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "controltower:GetBaseline"
      ],
      "Resource" : "arn:aws:controltower:*::baseline/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "ControlTowerEnableControlWithRequestTag",
      "Effect" : "Allow",
      "Action" : [
        "controltower:EnableControl"
      ],
      "Resource" : "arn:aws:controltower:*:*:enabledcontrol/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ControlTowerEnableBaselineAndOrganizationsAccountCreate",
      "Effect" : "Allow",
      "Action" : [
        "controltower:EnableBaseline",
        "controltower:TagResource",
        "organizations:CreateAccount"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "OrganizationsTagAndCreateOrganizationalUnit",
      "Effect" : "Allow",
      "Action" : [
        "organizations:CreateOrganizationalUnit",
        "organizations:TagResource"
      ],
```

```
      "Resource" : [
        "arn:aws:organizations::*:account/o-*/*",
        "arn:aws:organizations::*:ou/o-*/*",
        "arn:aws:organizations::*:policy/o-*/*",
        "arn:aws:organizations::*:root/o-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "OrganizationsResourceDescribeReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/*",
        "arn:aws:organizations::*:ou/*",
        "arn:aws:organizations::*:policy/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "OrganizationsPolicyUpdateViaControlTower",
      "Effect" : "Allow",
      "Action" : [
        "organizations:UpdatePolicy"
      ],
      "Resource" : "arn:aws:organizations::*:policy/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "controltower.amazonaws.com"
        },
```

```
        "StringEquals" : {
          "organizations:PolicyType" : "SERVICE_CONTROL_POLICY",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "OrganizationsHierarchyOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/*",
        "arn:aws:organizations::*:ou/*",
        "arn:aws:organizations::*:root/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "OrganizationsMoveAccountWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "organizations:MoveAccount"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/*",
        "arn:aws:organizations::*:ou/*",
        "arn:aws:organizations::*:root/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "OrganizationsListTagsForResource",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/o-*/*",
        "arn:aws:organizations::*:ou/o-*/*",
        "arn:aws:organizations::*:policy/o-*/*",
        "arn:aws:organizations::*:root/o-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "OrganizationsServiceControlPolicyCreateViaControlTower",
      "Effect" : "Allow",
      "Action" : [
        "organizations:CreatePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "controltower.amazonaws.com"
        },
        "StringEquals" : {
          "organizations:PolicyType" : "SERVICE_CONTROL_POLICY"
        }
      }
    },
    {
      "Sid" : "OrganizationsServiceControlPolicyAttachViaControlTower",
      "Effect" : "Allow",
      "Action" : [
        "organizations:AttachPolicy"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/o-*/*",
        "arn:aws:organizations::*:ou/o-*/*",
        "arn:aws:organizations::*:policy/o-*/*",
```

```
        "arn:aws:organizations::*:root/o-*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "controltower.amazonaws.com"
        },
        "StringEquals" : {
          "organizations:PolicyType" : "SERVICE_CONTROL_POLICY",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ServiceCatalogProvisioningArtifactOperations",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:DeleteProvisioningArtifact",
        "servicecatalog:ListProvisioningArtifacts",
        "servicecatalog:UpdateProvisioningArtifact"
      ],
      "Resource" : "arn:aws:catalog:*:*:product/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransformNetworkMigrationAgentPolicy

Descrição: Concede permissões ao AWS Transform para implantar e configurar a infraestrutura de rede, incluindo VPCs, Transit Gateways e tabelas de rotas para migração de rede

`AWSTransformNetworkMigrationAgentPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTransformNetworkMigrationAgentPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 06 de agosto de 2026, 15:27 UTC
- Horário editado: 01 de setembro de 2026, 10:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformNetworkMigrationAgentPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnNetworkMigrationStackCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnNetworkMigrationStackDescribeStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnNetworkMigrationStackListStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "CfnNetworkMigrationStackOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudformation:UpdateStack",
```

```
        "cloudformation:UpdateTerminationProtection"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "Ec2NetworkProvisionCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:CreateInternetGateway",
        "ec2:CreateTransitGateway",
        "ec2:CreateVpc"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "Ec2NetworkTopologyOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:GetSubnetCidrReservations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
```

```
        }
      }
    },
    {
      "Sid" : "Ec2TagOnCreateNetworkMigration",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:network-insights-access-scope-analysis/*",
        "arn:aws:ec2:*:*:network-insights-access-scope/*",
        "arn:aws:ec2:*:*:network-insights-analysis/*",
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group-rule/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:transit-gateway-connect-peer/*",
        "arn:aws:ec2:*:*:transit-gateway-policy-table/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : [
            "AllocateAddress",
            "CreateInternetGateway",
            "CreateNatGateway",
            "CreateNetworkInsightsAccessScope",
            "CreateNetworkInsightsPath",
            "CreateNetworkInterface",
            "CreateRouteTable",
            "CreateSecurityGroup",
            "CreateSubnet",
```

```
            "CreateTransitGateway",
            "CreateTransitGatewayConnect",
            "CreateTransitGatewayConnectPeer",
            "CreateTransitGatewayPeeringAttachment",
            "CreateTransitGatewayPolicyTable",
            "CreateTransitGatewayPrefixListReference",
            "CreateTransitGatewayRoute",
            "CreateTransitGatewayRouteTable",
            "CreateTransitGatewayRouteTableAnnouncement",
            "CreateTransitGatewayVpcAttachment",
            "CreateVpc",
            "StartNetworkInsightsAnalysis"
          ]
        }
      }
    },
    {
      "Sid" : "Ec2ViaCfnCrossOrgTgwAttachmentCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        }
      }
    },
    {
      "Sid" : "Ec2ViaCfnNetworkOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:AcceptTransitGatewayVpcAttachment",
        "ec2:AssociateNatGatewayAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTransitGateway",
        "ec2:DeleteTransitGatewayRoute",
        "ec2:DeleteTransitGatewayRouteTable",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DisableTransitGatewayRouteTablePropagation",
        "ec2:DisassociateNatGatewayAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyTransitGateway",
        "ec2:ModifyTransitGatewayVpcAttachment",
        "ec2:ModifyVpcAttribute",
        "ec2:RejectTransitGatewayVpcAttachment",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceTransitGatewayRoute",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "Ec2ViaCfnNetworkProvisionCreateWithRequestTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInsightsPath",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "Ec2ViaCfnNetworkProvisionCreateWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInsightsPath",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "ec2:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "Ec2ViaCfnOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "Ec2ViaCfnSecurityGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
```

```
        }
      }
    },
    {
      "Sid" : "Ec2ViaCfnSecurityGroupTagCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group-rule/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IamTgwServiceLinkedRoleCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/transitgateway.amazonaws.com/
AWSServiceRoleForVPCTransitGateway",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "iam:AWSServiceName" : "transitgateway.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "IamViaCfnTgwLambdaRoleCleanupOperations",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "IamViaCfnTgwLambdaRoleCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IamViaCfnTgwLambdaRoleOperationsReadOnly",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IamViaCfnTgwLambdaRolePassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IamViaCfnTgwLambdaRolePolicyAttach",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ArnEquals" : {
```

```
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/
AWSApplicationMigrationNetworkMigrationCustomResource",
            "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "IamViaCfnTgwLambdaRoleTag",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "KmsS3EncryptionOperationsNetworkMigration",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
```

```
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/EncryptionKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LambdaViaCfnNetworkMigrationFunctionCreate",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:network-migration*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaViaCfnNetworkMigrationFunctionOperations",
      "Effect" : "Allow",
      "Action" : [
        "lambda:DeleteFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:network-migration*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
```

```
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "LambdaViaCfnNetworkMigrationFunctionReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:ListTags"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:network-migration*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaViaCfnNetworkMigrationFunctionTag",
      "Effect" : "Allow",
      "Action" : [
        "lambda:TagResource"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:network-migration*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
```

```
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "LogsViaCfnNetworkMigrationOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/network-migration*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MgnNetworkMigrationDefinitionCreate",
      "Effect" : "Allow",
      "Action" : [
        "mgn:CreateNetworkMigrationDefinition"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "MgnNetworkMigrationDefinitionDelete",
```

```
      "Effect" : "Allow",
      "Action" : [
        "mgn:DeleteNetworkMigrationDefinition"
      ],
      "Resource" : "arn:aws:mgn:*:*:network-migration-definition/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : [
            "AWSTransform",
            "QTransform"
          ]
        }
      }
    },
    {
      "Sid" : "MgnNetworkMigrationDefinitionOperations",
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetNetworkMigrationDefinition",
        "mgn:ListNetworkMigrationMappingUpdates",
        "mgn:StartNetworkMigrationMappingUpdate",
        "mgn:UpdateNetworkMigrationDefinition",
        "mgn:UpdateNetworkMigrationMapperSegment",
        "mgn:UpdateNetworkMigrationMapperSegmentConstruct"
      ],
      "Resource" : "arn:aws:mgn:*:*:network-migration-definition/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "MgnNetworkMigrationDefinitionTagOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "mgn:TagResource"
      ],
      "Resource" : "arn:aws:mgn:*:*:network-migration-definition/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "mgn:CreateAction" : "CreateNetworkMigrationDefinition"
        }
      }
    },
    {
      "Sid" : "NetworkMigrationOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "mgn:ListNetworkMigrationAnalyses",
        "mgn:ListNetworkMigrationAnalysisResults",
        "mgn:ListNetworkMigrationCodeGenerationSegments",
        "mgn:ListNetworkMigrationCodeGenerations",
        "mgn:ListNetworkMigrationDefinitions",
        "mgn:ListNetworkMigrationDeployedStacks",
        "mgn:ListNetworkMigrationDeployedStacksDeletions",
        "mgn:ListNetworkMigrationDeployments",
        "mgn:ListNetworkMigrationExecutions",
        "mgn:ListNetworkMigrationMapperSegmentConstructs",
        "mgn:ListNetworkMigrationMapperSegments",
        "mgn:ListNetworkMigrationExecutionArtifacts",
        "mgn:ListNetworkMigrationMappings"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "NetworkMigrationOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "mgn:StartNetworkMigrationAnalysis",
        "mgn:StartNetworkMigrationCodeGeneration",
        "mgn:StartNetworkMigrationDeployedStacksDeletion",
        "mgn:StartNetworkMigrationDeployment",
```

```
        "mgn:StartNetworkMigrationMapping"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "OrganizationsOperationsReadOnlyNetworkMigration",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RamShareCrossAccountOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "RamViaCfnShareAssociateOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
```

```
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService",
          "ram:RequestedResourceType" : [
            "ec2:TransitGateway",
            "ssm:Parameter"
          ]
        }
      }
    },
    {
      "Sid" : "RamViaCfnShareCreate",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "Bool" : {
          "ram:RequestedAllowsExternalPrincipals" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RamViaCfnShareOperations",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:DisassociateResourceShare",
        "ram:UpdateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "RamViaCfnShareTagOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "ReachabilityAnalyzerAnalysisStart",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-insights-analysis/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReachabilityAnalyzerCleanupOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "ReachabilityAnalyzerCreateWithRequestTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath",
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "ReachabilityAnalyzerCreateWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateNetworkInsightsPath",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "ReachabilityAnalyzerCrossOrgPathCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        }
      }
    },
    {
      "Sid" : "ReachabilityAnalyzerOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
```

```
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
```

```
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "ReachabilityAnalyzerProbeCreateOnSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReachabilityAnalyzerSecurityGroupCreateOnVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
```

```
    {
      "Sid" : "ReachabilityAnalyzerSecurityGroupCreateWithRequestTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group-rule/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3TargetBucketOperationsNetworkMigration",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:ListBucket",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::transform-vmware-target-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3TargetObjectOperationsNetworkMigration",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
```

```
        "s3:GetObjectAttributes",
        "s3:GetObjectVersion",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::transform-vmware-target-*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SsmParametersViaCfnOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/network-migration/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "SsmParametersViaCfnOperationsWriteWithRequestTag",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/network-migration/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
```

```
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "SsmParametersViaCfnOperationsWriteWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:DeleteResourcePolicy",
        "ssm:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/network-migration/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "SsmParametersViaCfnRamSharingOperations",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetResourcePolicies",
        "ssm:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/network-migration/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
```

```
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "StsCrossAccountAssumeRoleNetworkMigration",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSTransformNetworkMigrationAgentSharingRole_
${aws:PrincipalAccount}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}",
          "sts:ExternalId" : "${aws:PrincipalAccount}:workspace/${aws:PrincipalTag/
WorkspaceId}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransformRevenueAttributionPolicy

Descrição: permite que o serviço AWS Transform gerencie a atribuição de receita do cliente para incentivos.

`AWSTransformRevenueAttributionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTransformRevenueAttributionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 07 de julho de 2026, 16:42 UTC
- Horário editado: 07 de julho de 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformRevenueAttributionPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PartnerCentralRevenueManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetRevenueAttribution",
        "partnercentral:UpdateRevenueAttribution",
        "partnercentral:CreateRevenueAttribution",
        "partnercentral:ListRevenueAttributions"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/revenue-attribution/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
```

```
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransformSecretsManagerConnectorPolicy

Descrição: permite que o serviço AWS Transform leia um SecretsManager segredo especificado em conexão com a chave KMS especificada. Essa política concede permissões para ler o valor secreto especificado e descriptografá-lo se o segredo estiver criptografado.

`AWSTransformSecretsManagerConnectorPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTransformSecretsManagerConnectorPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 04 de março de 2026, 21:12 UTC
- Horário editado: 04 de março de 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformSecretsManagerConnectorPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadSecretsManagerSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:${aws:PrincipalTag/SecretId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DecryptWithCustomerProvidedKMSKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KMSKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:
${aws:RequestedRegion}:${aws:PrincipalAccount}:secret:${aws:PrincipalTag/SecretId}",
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DescribeKMSKey",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransformSecurityAgentExecutorAccess

Descrição: Concede à modernização contínua do AWS Transform (ATX) as permissões necessárias para invocar CLI/agent o serviço AWS Security Agent para análises e correções automatizadas de segurança de código, incluindo o upload de artefatos de digitalização e a recuperação de descobertas.

`AWSTransformSecurityAgentExecutorAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTransformSecurityAgentExecutorAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 30 de junho de 2026, 21:27 UTC

- Horário editado: 28 de julho de 2026, 15:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformSecurityAgentExecutorAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityAgentApi",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:ListAgentSpaces",
        "securityagent:CreateCodeReview",
        "securityagent:StartCodeReviewJob",
        "securityagent:ListCodeReviewJobsForCodeReview",
        "securityagent:ListFindings",
        "securityagent:BatchGetFindings",
        "securityagent:StartCodeRemediation"
      ],
      "Resource" : "arn:aws:securityagent:*:*:agent-space*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3SecurityAgentBucketRead",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::atx-security-agent-*",
        "arn:aws:s3:::atx-security-agent-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3SecurityAgentUpload",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : "arn:aws:s3:::atx-security-agent-*/security-scans/*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassSecurityAgentRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/security-agent-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "securityagent.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CFNDiscoverSecurityAgentStack",
      "Effect" : "Allow",
      "Action" : "cloudformation:ListStacks",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "CFNDescribeSecurityAgentStack",
      "Effect" : "Allow",
      "Action" : "cloudformation:DescribeStacks",
      "Resource" : "arn:aws:cloudformation:*:*:stack/AtxSecurityAgentStack-*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTransformServerMigrationAgentPolicy

Descrição: Concede permissões ao AWS Transform para realizar operações de migração de servidor, incluindo replicação, teste e transferência usando AWS o Application Migration Service

`AWSTransformServerMigrationAgentPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTransformServerMigrationAgentPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 06 de agosto de 2026, 15:27 UTC
- Horário editado: 01 de setembro de 2026, 10:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformServerMigrationAgentPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2LaunchTemplateOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "Ec2OperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "Ec2TagOnCreateServerMigration",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnInstanceLifecycleOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateSnapshot",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteVolume",
        "ec2:DetachVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnInstanceProvisionCreateWithRequestTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateVolume",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
```

```
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnLaunchOnSharedVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedFor" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnLaunchOnWorkspaceVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedFor" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:GetSubnetCidrReservations",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
```

```
      "Sid" : "Ec2ViaMgnRunInstancesOnAmsSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnRunInstancesOnImage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnRunInstancesOnSg",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnSecurityGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnTagOnCreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateSnapshot",
            "CreateVolume",
```

```
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "Ec2ViaMgnVolumeFromSnapshotCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "ec2:Owner" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FsxOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "FsxViaMgnDescribeOperations",
      "Effect" : "Allow",
```

```
      "Action" : [
        "fsx:DescribeVolumes",
        "fsx:DescribeSnapshots"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "FsxViaMgnCreateVolume",
      "Effect" : "Allow",
      "Action" : "fsx:CreateVolume",
      "Resource" : [
        "arn:aws:fsx:*:*:volume/*/*",
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FsxViaMgnDeleteVolumeAndTag",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteVolume",
```

```
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FsxViaMgnCreateSnapshot",
      "Effect" : "Allow",
      "Action" : "fsx:CreateSnapshot",
      "Resource" : [
        "arn:aws:fsx:*:*:snapshot/*/*",
        "arn:aws:fsx:*:*:volume/*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IamViaMgnEc2PassRole",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithDrsRole",
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KmsS3EncryptionOperationsServerMigration",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/EncryptionKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "MgnAccountSettingsOperations",
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetAccountSettings",
        "mgn:RegisterAgentForMgn",
        "mgn:UpdateAccountSettings"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "MgnAppWaveCreate",
      "Effect" : "Allow",
      "Action" : [
        "mgn:CreateApplication",
        "mgn:CreateWave"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "MgnAppWaveServerTagOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "mgn:TagResource"
      ],
      "Resource" : [
        "arn:aws:mgn:*:*:application/*",
        "arn:aws:mgn:*:*:source-server/*",
        "arn:aws:mgn:*:*:wave/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
```

```
    },
    {
      "Sid" : "MgnImportExportOperationWrite",
      "Effect" : "Allow",
      "Action" : [
        "mgn:StartExport",
        "mgn:StartImport",
        "mgn:StartImportFileEnrichment"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "MgnImportExportTagOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "mgn:TagResource"
      ],
      "Resource" : [
        "arn:aws:mgn:*:*:export/*",
        "arn:aws:mgn:*:*:import/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "mgn:CreateAction" : [
            "StartExport",
            "StartImport"
          ]
        }
      }
    },
    {
      "Sid" : "MgnJobAndErrorOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "mgn:DescribeJobLogItems",
```

```
        "mgn:ListExportErrors",
        "mgn:ListImportErrors"
      ],
      "Resource" : [
        "arn:aws:mgn:*:*:export/*",
        "arn:aws:mgn:*:*:import/*",
        "arn:aws:mgn:*:*:job/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "MgnJobTagOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "mgn:TagResource"
      ],
      "Resource" : "arn:aws:mgn:*:*:job/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "mgn:CreateAction" : [
            "StartCutover",
            "StartTest",
            "TerminateTargetInstances"
          ]
        }
      }
    },
    {
      "Sid" : "MgnSourceServerLifecycleOperations",
      "Effect" : "Allow",
      "Action" : [
        "mgn:ChangeServerLifecycleState",
        "mgn:FinalizeCutover",
```

```
        "mgn:GetReplicationConfiguration",
        "mgn:ListSourceServerActions",
        "mgn:ListTagsForResource",
        "mgn:MarkAsArchived",
        "mgn:PauseReplication",
        "mgn:PutSourceServerAction",
        "mgn:RemoveSourceServerAction",
        "mgn:ResumeReplication",
        "mgn:StartCutover",
        "mgn:StartReplication",
        "mgn:StartTest",
        "mgn:StopReplication",
        "mgn:UpdateReplicationConfiguration",
        "mgn:UpdateSourceServer"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "OrganizationsOperationsReadOnlyServerMigration",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PostLaunchAutomationMonitoring",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
```

```
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AgentSignatureOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::aws-application-migration-service-*/latest/source-
automation-client/linux/ssaf-client/ssaf_client.sig"
    },
    {
      "Sid" : "S3TargetBucketOperationsServerMigration",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:ListBucket",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::transform-vmware-target-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3TargetObjectOperationsServerMigration",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAttributes",
```

```
        "s3:GetObjectVersion",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::transform-vmware-target-*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "ServerMigrationOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "mgn:DescribeJobs",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:DescribeReplicationServerAssociationsForMgn",
        "mgn:DescribeSourceServers",
        "mgn:DescribeVcenterClients",
        "mgn:GetLaunchConfiguration",
        "mgn:ListApplications",
        "mgn:ListConnectors",
        "mgn:ListExports",
        "mgn:ListImportFileEnrichments",
        "mgn:ListImports",
        "mgn:ListTemplateActions",
        "mgn:ListWaves"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "ServerMigrationOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "mgn:AssociateApplications",
        "mgn:AssociateSourceServers",
        "mgn:DeleteApplication",
        "mgn:DeleteWave",
        "mgn:DisassociateApplications",
        "mgn:DisassociateSourceServers",
        "mgn:TerminateTargetInstances",
        "mgn:UpdateApplication",
        "mgn:UpdateLaunchConfiguration",
        "mgn:UpdateWave"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "ServerMigrationTemplateOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "mgn:PutTemplateAction",
        "mgn:RemoveTemplateAction",
        "mgn:UpdateLaunchConfigurationTemplate",
        "mgn:UpdateReplicationConfigurationTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ServiceQuotasViaMgnOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "arn:aws:servicequotas:*:*:vpc/L-2AFB9258",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SsmAgentCommandOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "SsmAgentCommandOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
```

```
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedFor" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "SsmDocumentListOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "SsmDocumentOnAwsManagedOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument",
        "ssm:ListDocumentVersions"
      ],
      "Resource" : "arn:aws:ssm:*::document/AWS*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "SsmDocumentOperationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
```

```
        "ssm:GetDocument",
        "ssm:ListDocumentVersions"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SsmMigrationDocumentOperations",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:SendCommand"
      ],
      "Resource" : "arn:aws:ssm:*::document/AWSMigration-RunSourceServerAction",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
    },
    {
      "Sid" : "SsmParameterServerMigrationOperationsWrite",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameters",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "SsmViaMgnPostLaunchCommandAndAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/*:*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SsmViaMgnPostLaunchCommandAndAutomationOnAwsManaged",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*::automation-definition/AWS*:*",
        "arn:aws:ssm:*::document/AWS*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}"
        }
      }
```

```
    },
    {
      "Sid" : "SsmViaMgnPostLaunchSendCommandToInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "StringEquals" : {
          "aws:RequestedRegion" : "${aws:PrincipalTag/TargetRegion}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/ATWorkspace" : "${aws:PrincipalTag/WorkspaceId}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Sid" : "StsCrossAccountAssumeRole",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSTransformRehostSharingRole_
${aws:PrincipalAccount}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}",
          "sts:ExternalId" : "${aws:PrincipalAccount}:workspace/${aws:PrincipalTag/
WorkspaceId}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTrustedAdvisorPriorityFullAccess

Descrição: Fornece acesso total ao AWS Trusted Advisor Priority. Essa política também permite que o usuário adicione o Trusted Advisor como um serviço confiável com AWS organizações e especifique contas de administrador delegadas para a prioridade do Trusted Advisor.

`AWSTrustedAdvisorPriorityFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTrustedAdvisorPriorityFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 16 de agosto de 2022, 16:08 UTC
- Hora da edição: 16 de agosto de 2022, 16:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeAccount*",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:DownloadRisk",
        "trustedadvisor:UpdateRiskStatus",
        "trustedadvisor:DescribeNotificationConfigurations",
        "trustedadvisor:UpdateNotificationConfigurations",
        "trustedadvisor:DeleteNotificationConfigurationForDelegatedAdmin",
        "trustedadvisor:SetOrganizationAccess"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "reporting.trustedadvisor.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTrustedAdvisorPriorityReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao AWS Trusted Advisor Priority. Isso inclui permissão para visualizar as contas de administrador delegado.

`AWSTrustedAdvisorPriorityReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSTrustedAdvisorPriorityReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 16 de agosto de 2022, 16:35 UTC
- Hora da edição: 16 de agosto de 2022, 16:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeAccount*",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:DownloadRisk",
```

```
        "trustedadvisor:DescribeNotificationConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTrustedAdvisorReportingServiceRolePolicy

Descrição: Política de serviço para Multi-account relatórios do Trusted Advisor

`AWSTrustedAdvisorReportingServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 19 de novembro de 2019, 17:41 UTC
- Hora da edição: 28 de fevereiro de 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit",
```

```
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSTrustedAdvisorServiceRolePolicy

Descrição: Acesso ao AWS Trusted Advisor Service para ajudar a reduzir custos, aumentar o desempenho e melhorar a segurança do seu AWS ambiente.

`AWSTrustedAdvisorServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 22 de fevereiro de 2018, 21:24 UTC
- Horário editado: 14 de maio de 2026, 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedAdvisorServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudfront:ListDistributions",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "dax:DescribeClusters",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeImages",
        "ec2:DescribeNatGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:GetManagedPrefixListEntries",
        "ecs:DescribeTaskDefinition",
        "ecs:ListTaskDefinitions",
        "ecs:ListClusters",
        "ecs:ListTasks",
        "ecs:DescribeTasks",
        "ecs:ListTaskDefinitionFamilies",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "iam:GenerateCredentialReport",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetServerCertificate",
        "iam:ListServerCertificates",
        "iam:ListSAMLProviders",
        "kinesis:DescribeLimits",
        "kafka:DescribeClusterV2",
        "kafka:ListClustersV2",
        "kafka:ListNodes",
        "network-firewall:ListFirewalls",
        "network-firewall:DescribeFirewall",
        "outposts:ListAssets",
        "outposts:GetOutpost",
        "outposts:ListOutposts",
        "rds:DescribeAccountAttributes",
        "rds:DescribeDBClusters",
```

```
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroupOptions",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribeReservedDBInstances",
        "rds:DescribeReservedDBInstancesOfferings",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeReservedNodeOfferings",
        "redshift:DescribeReservedNodes",
        "route53:GetAccountLimit",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetLifecycleConfiguration",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "ses:GetSendQuota",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSUserAttributeCostAllocationPolicy

Descrição: fornece acesso somente para leitura aos atributos do usuário do AWS IAM Identity Center para os atributos do usuário que o cliente optou por usar.

`AWSUserAttributeCostAllocationPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 15 de dezembro de 2025, 16:34 UTC
- Horário editado: 15 de dezembro de 2025, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserAttributeCostAllocationPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/user-attribute-cost-
allocation-data.amazonaws.com/AWSServiceRoleForUserAttributeCostAllocation"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSUserNotificationsServiceLinkedRolePolicy

Descrição: permite que as notificações AWS do usuário liguem para AWS os serviços em seu nome.

`AWSUserNotificationsServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 19 de abril de 2023, 13:28 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:ListTargetsByRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AWSUserNotificationsManagedRule-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Notifications"
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrgsActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
```

```
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListParents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAdminDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "notifications.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationNotificationConfigurationDistribution",
      "Effect" : "Allow",
      "Action" : [
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteNotificationConfiguration",
        "notifications:CreateEventRule",
        "notifications:UpdateEventRule",
        "notifications:DeleteEventRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSVendorInsightsAssessorFullAccess

Descrição: fornece acesso total para visualização de recursos autorizados do Vendor Insights e gerenciamento de assinaturas do Vendor Insights

`AWSVendorInsightsAssessorFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSVendorInsightsAssessorFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de julho de 2022, 15:05 UTC
- Hora da edição: 01 de dezembro de 2022, 0:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetProfileAccessTerms",
        "vendor-insights:ListEntitledSecurityProfiles",
```

```
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:CancelAgreement"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSVendorInsightsAssessorReadOnly

Descrição: fornece acesso somente leitura para visualizar recursos autorizados do Vendor Insights

`AWSVendorInsightsAssessorReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSVendorInsightsAssessorReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de julho de 2022, 15:05 UTC
- Hora da edição: 01 de dezembro de 2022, 0:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSVendorInsightsVendorFullAccess

Descrição: fornece acesso total para criar e gerenciar os recursos do Vendor Insights

`AWSVendorInsightsVendorFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSVendorInsightsVendorFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de julho de 2022, 15:05 UTC
- Hora da edição: 19 de outubro de 2023, 1:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:DescribeEntity",
      "Resource" : "arn:aws:aws-marketplace:*:*:*/SaaSProduct/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:ListEntities",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:CreateDataSource",
        "vendor-insights:UpdateDataSource",
        "vendor-insights:DeleteDataSource",
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:CreateSecurityProfile",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:AssociateDataSource",
        "vendor-insights:DisassociateDataSource",
        "vendor-insights:UpdateSecurityProfile",
        "vendor-insights:ActivateSecurityProfile",
        "vendor-insights:DeactivateSecurityProfile",
        "vendor-insights:UpdateSecurityProfileSnapshotCreationConfiguration",
        "vendor-insights:UpdateSecurityProfileSnapshotReleaseConfiguration",
        "vendor-insights:ListSecurityProfileSnapshots",
        "vendor-insights:GetSecurityProfileSnapshot",
```

```
        "vendor-insights:TagResource",
        "vendor-insights:UntagResource",
        "vendor-insights:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:CancelAgreement",
        "aws-marketplace:SearchAgreements"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSVendorInsightsVendorReadOnly

Descrição: fornece acesso somente leitura para visualizar os recursos do Vendor Insights

`AWSVendorInsightsVendorReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSVendorInsightsVendorReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 26 de julho de 2022, 15:05 UTC
- Hora da edição: 01 de dezembro de 2022, 0:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:DescribeEntity",
      "Resource" : "arn:aws:aws-marketplace:*:*:*/SaaSProduct/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:ListEntities",
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots",
        "vendor-insights:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSVPCFlowLogsServiceRolePolicy

Descrição: fornece permissões para controlar os recursos gerenciados pelo serviço e as APIs de chamadas necessárias para o enriquecimento do campo de registro em nome dos clientes.

`AWSVPCFlowLogsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 11 de maio de 2026, 15:57 UTC
- Horário editado: 11 de maio de 2026, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCFlowLogsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutRuleOnSpecificSourcesAndDetailTypes",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : [
        "arn:aws:events:*:*:rule/VPCFlowLogsEC2TagsManagedRule",
        "arn:aws:events:*:*:rule/VPCFlowLogsASGTagsManagedRule"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.tag",
            "aws.autoscaling"
```

```
          ],
          "events:detail-type" : [
            "AWS API Call via CloudTrail",
            "Tag Change on Resource"
          ]
        },
        "Null" : {
          "events:source" : "false",
          "events:detail-type" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowOtherOperationsOnRulesManagedByVPCFlowLogs",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/VPCFlowLogsEC2TagsManagedRule",
        "arn:aws:events:*:*:rule/VPCFlowLogsASGTagsManagedRule"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeTagsOnAllEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "autoscaling:DescribeTags"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSVpcLatticeServiceRolePolicy

Descrição: permite que o VPC Lattice acesse AWS recursos em seu nome.

`AWSVpcLatticeServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 30 de novembro de 2022, 20:47 UTC
- Horário editado: 01 de dezembro de 2024, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/VpcLattice"
        }
      }
    },
    {
      "Sid" : "VpcLatticeDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcLatticeCreateNetworkInterfaceWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/VpcLatticeManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VpcLatticeCreateNetworkInterfaceWithSubnetAndSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
```

```
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "VpcLatticeTagNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "VpcLatticeMutateNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VpcLatticeManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VpcLatticeModifyNetworkInterfaceSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "VpcLatticeModifyNetworkInterfaceActionsIpAddressActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
```

```
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VpcLatticeManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VpcLatticeAssociateHostedZoneToVpc",
      "Effect" : "Allow",
      "Action" : [
        "route53:AssociateVPCWithHostedZone"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSVPCS2SVpnServiceRolePolicy

Descrição: Permita que a Site-to-Site VPN crie e gerencie recursos relacionados às suas conexões VPN.

`AWSVPCS2SVpnServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 06 de agosto de 2019, 14:13 UTC
- Horário editado: 15 de maio de 2025, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpnConnectionSecretsManagement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
```

```
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:s2svpn!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "s2svpn",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "VpnConnectionSecretsCreation",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:s2svpn!*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "s2svpn!*"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSVPCTransitGatewayServiceRolePolicy

Descrição: permite que o gateway de trânsito da VPC crie e gerencie os recursos necessários para os anexos da sua VPC do Transit Gateway.

`AWSVPCTransitGatewayServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 26 de novembro de 2018, 16:21 UTC
- Hora da edição: 15 de abril de 2021, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AssignIpv6Addresses",
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "*",
      "Effect" : "Allow",
      "Sid" : "0"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSVPCVerifiedAccessServiceRolePolicy

Descrição: Política para permitir que o serviço de Acesso AWS Verificado provisione endpoints em seu nome

`AWSVPCVerifiedAccessServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 29 de novembro de 2022, 3:35 UTC
- Hora da edição: 17 de novembro de 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "VerifiedAccessRoleModifyTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VerifiedAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VerifiedAccessRoleModifyNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "VerifiedAccessRoleNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "VerifiedAccessRoleTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/VerifiedAccessManaged" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "VerifiedAccessRoleTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSWAFConsoleFullAccess

Descrição: Fornece acesso total ao AWS WAF por meio do Console de gerenciamento da AWS. Observe que essa política também concede permissões para listar e atualizar CloudFront distribuições da Amazon, permissões para visualizar balanceadores de carga no AWS Elastic Load Balancing, permissões para visualizar APIs e estágios REST do Amazon API Gateway, permissões para listar e visualizar CloudWatch métricas da Amazon e permissões para visualizar regiões habilitadas na conta.

`AWSWAFConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSWAFConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de abril de 2020, 18:38 UTC
- Horário editado: 01 de julho de 2026, 04:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess`

Versão da política

Versão da política: v22 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:*",
        "waf-regional:*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
```

```
        "arn:aws:waf:*:*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:*"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowDisassociateWebACL",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:DisassociateWebACL"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2DescribeRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetDistribution",
        "cloudfront:UpdateDistribution",
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:DisassociateDistributionWebACL"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFront",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionTenant",
        "cloudfront:AssociateDistributionTenantWebACL",
        "cloudfront:DisassociateDistributionTenantWebACL"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution-tenant/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListDistributionTenantsByCustomization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:SetWebAcl",
        "elasticloadbalancing:CreateWebACLAssociation",
        "elasticloadbalancing:DeleteWebACLAssociation",
        "elasticloadbalancing:GetLoadBalancerWebACL"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowListActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeWebACLAssociation"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:SetWebACL"
      ],
      "Resource" : "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
    {
      "Sid" : "AllowListActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "arn:aws:apigateway:*::/*"
    },
    {
      "Sid" : "AllowActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:SetWebACL",
        "appsync:AssociateWebACL",
        "appsync:DisassociateWebACL",
        "appsync:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListGraphqlApis",
        "appsync:ListApis",
        "appsync:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:GetWebACLForResource"
```

```
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListUserPools",
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:AssociateWebACL",
        "amplify:DisassociateWebACL",
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogQueryActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:DescribeQueryDefinitions",
        "logs:GetQueryResults"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:aws-waf-logs-*"
    },
    {
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowLogDeliverySubscription",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowListActionForFirehoseStream",
      "Effect" : "Allow",
      "Action" : [
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowActionsForPricing",
      "Effect" : "Allow",
      "Action" : [
        "pricing:ListPriceLists",
        "pricing:GetPriceListFileUrl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:GetSubscription",
        "pricingplanmanager:UpdateSubscription",
        "pricingplanmanager:CancelSubscription",
        "pricingplanmanager:CancelSubscriptionChange"
      ],
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
    },
    {
      "Sid" : "AllowListActionsForRoute53",
      "Effect" : "Allow",
      "Action" : [
        "route53:ListHostedZones",
        "route53:GetHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : "pricingplanmanager:ListSubscriptions",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAgentCoreGateway",
```

```
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayAssociateWebACL",
        "bedrock-agentcore:GatewayDisassociateWebACL",
        "bedrock-agentcore:GatewayGetWebACLForResource",
        "bedrock-agentcore:GetGateway"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:gateway/*"
    },
    {
      "Sid" : "AllowListActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayListResourcesForWebACL",
        "bedrock-agentcore:ListGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSWAFConsoleReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao AWS WAF por meio do. Console de gerenciamento da AWS Observe que essa política também concede permissões para listar CloudFront distribuições da Amazon, permissões para visualizar balanceadores de carga no AWS Elastic Load Balancing, permissões para visualizar APIs e estágios REST do Amazon API Gateway, permissões para listar e visualizar CloudWatch métricas da Amazon e permissões para visualizar regiões habilitadas na conta.

`AWSWAFConsoleReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSWAFConsoleReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de abril de 2020, 18:43 UTC
- Horário editado: 01 de julho de 2026, 04:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess`

Versão da política

Versão da política: v21 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
```

```
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf:*:*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowReadOnlyOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:Describe*",
        "wafv2:CheckCapacity"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
```

```
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowEC2DescribeRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionTenant"
```

```
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution-tenant/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListDistributionTenantsByCustomization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:GetLoadBalancerWebACL"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowListActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeWebACLAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "arn:aws:apigateway:*::/*"
    },
    {
      "Sid" : "AllowGetActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
```

```
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListGraphqlApis",
        "appsync:ListApis",
        "appsync:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListUserPools",
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowGetActionForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionForFirehoseStream",
      "Effect" : "Allow",
      "Action" : [
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForPricing",
      "Effect" : "Allow",
      "Action" : [
        "pricing:ListPriceLists",
        "pricing:GetPriceListFileUrl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogQueryActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:DescribeQueryDefinitions",
        "logs:GetQueryResults"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:aws-waf-logs-*"
    },
    {
```

```
      "Sid" : "AllowListActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:GetSubscription"
      ],
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
    },
    {
      "Sid" : "AllowListActionsForRoute53",
      "Effect" : "Allow",
      "Action" : [
        "route53:ListHostedZones",
        "route53:GetHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListSubscriptionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:ListSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayGetWebACLForResource",
        "bedrock-agentcore:GetGateway"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:gateway/*"
    },
    {
      "Sid" : "AllowListActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayListResourcesForWebACL",
        "bedrock-agentcore:ListGateways"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSWAFFullAccess

Descrição: Fornece acesso total às ações do AWS WAF.

`AWSWAFFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSWAFFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de outubro de 2015, 20:44 UTC
- Horário editado: 28 de julho de 2026, 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFFullAccess`

Versão da política

Versão da política: v17 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:*",
        "waf-regional:*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf::*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
```

```
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:*"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowDisassociateWebACL",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeWebACLAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:SetWebAcl",
        "elasticloadbalancing:CreateWebACLAssociation",
        "elasticloadbalancing:DeleteWebACLAssociation",
        "elasticloadbalancing:GetLoadBalancerWebACL"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
```

```
      "Sid" : "AllowActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:SetWebACL"
      ],
      "Resource" : "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:SetWebACL",
        "appsync:AssociateWebACL",
        "appsync:DisassociateWebACL",
        "appsync:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:AssociateWebACL",
        "amplify:DisassociateWebACL",
        "amplify:GetWebACLForResource"
```

```
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogDeliverySubscription",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayAssociateWebACL",
        "bedrock-agentcore:GatewayDisassociateWebACL",
        "bedrock-agentcore:GatewayGetWebACLForResource"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:gateway/*"
    },
    {
      "Sid" : "AllowListActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayListResourcesForWebACL"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSWAFReadOnlyAccess

Descrição: Fornece acesso somente para leitura às ações do AWS WAF.

`AWSWAFReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSWAFReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de outubro de 2015, 20:43 UTC
- Horário editado: 01 de julho de 2026, 04:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess`

Versão da política

Versão da política: v13 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*"
      ],
      "Resource" : [
```

```
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf::*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowReadOnlyOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:Describe*",
        "wafv2:CheckCapacity"
```

```
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowGetActionForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAVA",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListResourcesForWebACL"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionsForELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:GetLoadBalancerWebACL"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowListActionsForELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeWebACLAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayGetWebACLForResource"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:gateway/*"
    },
    {
      "Sid" : "AllowListActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayListResourcesForWebACL"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSWellArchitectedAgentOrganizationsServiceRolePolicy

Descrição: permite que o AWS Well-Architected agente acesse a estrutura organizacional e as informações do administrador delegado nas AWS organizações em seu nome

`AWSWellArchitectedAgentOrganizationsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 15 de setembro de 2026, 18:37 UTC
- Horário editado: 15 de setembro de 2026, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedAgentOrganizationsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSWellArchitectedAgentResourceScanningServiceRolePolicy

Descrição: Concede ao AWS Well-Architected agente acesso somente para leitura às configurações de AWS recursos, configurações de segurança e dados operacionais para gerar recomendações de otimização

`AWSWellArchitectedAgentResourceScanningServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 04 de agosto de 2026, 17:27 UTC
- Horário editado: 24 de setembro de 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedAgentResourceScanningServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WellArchitectedAgentScanningReadOnly1",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "aco-automation:GetAutomationRule",
        "aco-automation:ListAutomationRules",
        "aidevops:DescribePrivateConnection",
        "aidevops:GetAgentSpace",
        "aidevops:GetAssociation",
        "aidevops:GetOperatorApp",
        "aidevops:GetService",
```

```
        "aidevops:ListAgentSpaces",
        "aidevops:ListAssociations",
        "aidevops:ListPrivateConnections",
        "aidevops:ListServices",
        "aidevops:ListTagsForResource",
        "aiops:GetInvestigationGroup",
        "aiops:GetInvestigationGroupPolicy",
        "aiops:ListInvestigationGroups",
        "aiops:ListTagsForResource",
        "airflow-serverless:GetWorkflow",
        "airflow-serverless:ListTagsForResource",
        "airflow-serverless:ListWorkflows",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListTagsForResource",
        "amplifyuibuilder:GetComponent",
        "amplifyuibuilder:GetForm",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListComponents",
        "amplifyuibuilder:ListForms",
        "amplifyuibuilder:ListThemes",
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "apigateway:GetRoutingRule",
        "apigateway:ListRoutingRules",
```

```
        "app-integrations:GetApplication",
        "app-integrations:GetDataIntegration",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListApplications",
        "app-integrations:ListDataIntegrations",
        "app-integrations:ListEventIntegrations",
        "app-integrations:ListTagsForResource",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtension",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListDeployments",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnector",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListConnectors",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListGroupingAttributeDefinitions",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource",
        "applicationinsights:DescribeApplication",
        "applicationinsights:DescribeComponent",
        "applicationinsights:DescribeLogPattern",
        "applicationinsights:ListApplications",
```

```
        "applicationinsights:ListComponents",
        "applicationinsights:ListLogPatternSets",
        "applicationinsights:ListLogPatterns",
        "applicationinsights:ListTagsForResource",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListServices",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:DescribeAppBlockBuilders",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appstream:DescribeUserStackAssociations",
        "appstream:DescribeUsers",
        "appstream:ListTagsForResource",
        "appsync:GetApi",
        "appsync:GetChannelNamespace",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetGraphqlApi",
        "appsync:GetSourceApiAssociation",
        "appsync:ListApis",
        "appsync:ListChannelNamespaces",
        "appsync:ListDataSources",
        "appsync:ListDomainNames",
        "appsync:ListFunctions",
        "appsync:ListGraphqlApis",
        "appsync:ListResolvers",
        "appsync:ListSourceApiAssociations",
        "appsync:ListTagsForResource",
        "apptest:GetTestCase",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeAnomalyDetector",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration",
        "aps:DescribeResourcePolicy",
```

```
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeScraperLoggingConfiguration",
        "aps:DescribeWorkspace",
        "aps:DescribeWorkspaceConfiguration",
        "aps:ListAnomalyDetectors",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "arc-region-switch:GetPlan",
        "arc-region-switch:ListPlans",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListTagsForResource",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:ListManagedResources",
        "athena:GetCapacityAssignmentConfiguration",
        "athena:GetCapacityReservation",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListCapacityReservations",
        "athena:ListDataCatalogs",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessments",
        "auditmanager:ListTagsForResource",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAccountSettings",
        "autoscaling:DescribeAdjustmentTypes",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeAutoScalingNotificationTypes",
        "autoscaling:DescribeInstanceRefreshes",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHookTypes",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribeLoadBalancerTargetGroups",
        "autoscaling:DescribeLoadBalancers",
```

```
        "autoscaling:DescribeMetricCollectionTypes",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScalingProcessTypes",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeTerminationPolicyTypes",
        "autoscaling:DescribeTrafficSources",
        "autoscaling:DescribeWarmPool",
        "aws-external-anthropic:GetWorkspace",
        "aws-external-anthropic:ListTagsForResource",
        "aws-external-anthropic:ListWorkspaces",
        "b2bi:GetCapability",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:GetTransformer",
        "b2bi:ListCapabilities",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "b2bi:ListTagsForResource",
        "b2bi:ListTransformers",
        "backup-gateway:GetHypervisor",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:GetTieringConfiguration",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListReportPlans",
        "backup:ListRestoreTestingPlans",
        "backup:ListRestoreTestingSelections",
        "backup:ListTags",
        "backup:ListTieringConfigurations",
```

```
        "batch:DescribeComputeEnvironments",
        "batch:DescribeConsumableResource",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobQueues",
        "batch:DescribeQuotaShare",
        "batch:DescribeSchedulingPolicies",
        "batch:DescribeServiceEnvironments",
        "batch:ListConsumableResources",
        "batch:ListQuotaShares",
        "batch:ListSchedulingPolicies",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:ListExports",
        "bcm-data-exports:ListTagsForResource",
        "bcm-pricing-calculator:GetBillScenario",
        "bcm-pricing-calculator:ListBillScenarios",
        "bcm-pricing-calculator:ListTagsForResource",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetBrowserProfile",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetDataset",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetHarness",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPaymentConnector",
        "bedrock-agentcore:GetPaymentCredentialProvider",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBrowserProfiles",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListDatasets",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListGatewayTargets",
```

```
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListHarnesses",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:ListPaymentConnectors",
        "bedrock-agentcore:ListPaymentCredentialProviders",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock-mantle:GetProject",
        "bedrock-mantle:ListProjects",
        "bedrock-mantle:ListTagsForResource",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAutomatedReasoningPolicy",
        "bedrock:GetBlueprint",
        "bedrock:GetDataAutomationLibrary",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataSource",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetPrompt",
        "bedrock:GetPromptRouter",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAutomatedReasoningPolicies",
        "bedrock:ListBlueprints",
        "bedrock:ListDataAutomationLibraries",
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListDataSources",
        "bedrock:ListEnforcedGuardrailsConfiguration",
        "bedrock:ListFlowAliases",
```

```
        "bedrock:ListFlowVersions",
        "bedrock:ListFlows",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "billing:GetBillingView",
        "billing:ListBillingViews",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItemVersions",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListResourcesAssociatedToCustomLineItem",
        "billingconductor:ListTagsForResource",
        "braket:ListTagsForResource",
        "braket:SearchSpendingLimits",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ListTagsForResource",
        "cases:BatchGetCaseRule",
        "cases:BatchGetField",
        "cases:GetDomain",
        "cases:GetLayout",
        "cases:GetTemplate",
        "cases:ListCaseRules",
        "cases:ListDomains",
        "cases:ListFields",
        "cases:ListLayouts",
        "cases:ListTemplates",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageWithResources",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
```

```
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:GetCustomAction",
        "chatbot:GetMicrosoftTeamsChannelConfiguration",
        "chatbot:ListAssociations",
        "chatbot:ListCustomActions",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chatbot:ListTagsForResource",
        "chime:DescribeAppInstance",
        "chime:DescribeAppInstanceBot",
        "chime:ListAppInstanceBots",
        "chime:ListAppInstances",
        "chime:ListTagsForResource",
        "cleanrooms-ml:GetConfiguredModelAlgorithm",
        "cleanrooms-ml:GetConfiguredModelAlgorithmAssociation",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListConfiguredModelAlgorithmAssociations",
        "cleanrooms-ml:ListConfiguredModelAlgorithms",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetConfiguredTableAssociationAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListTagsForResource",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribePublisher",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeType",
```

```
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSets",
        "cloudformation:ListStacks",
        "cloudformation:ListTypeVersions",
        "cloudformation:ListTypes",
        "cloudfront:DescribeConnectionFunction",
        "cloudfront:DescribeFunction",
        "cloudfront:DescribeKeyValueStore",
        "cloudfront:GetAnycastIpList",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetConnectionFunction",
        "cloudfront:GetConnectionGroup",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetDistributionTenant",
        "cloudfront:GetFunction",
        "cloudfront:GetKeyGroup",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:GetTrustStore",
        "cloudfront:GetVpcOrigin",
        "cloudfront:ListAnycastIpLists",
        "cloudfront:ListCachePolicies",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListConnectionFunctions",
        "cloudfront:ListConnectionGroups",
        "cloudfront:ListContinuousDeploymentPolicies",
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListDistributions",
        "cloudfront:ListFunctions",
        "cloudfront:ListKeyGroups",
        "cloudfront:ListKeyValueStores",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListPublicKeys",
```

```
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudfront:ListTrustStores",
        "cloudfront:ListVpcOrigins",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetChannel",
        "cloudtrail:GetDashboard",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListChannels",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetAlarmMuteRule",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricStream",
        "cloudwatch:GetMetricWidgetImage",
        "cloudwatch:GetOTelEnrichment",
        "cloudwatch:ListAlarmMuteRules",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListManagedInsightRules",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListMetrics",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackageGroup",
        "codeartifact:DescribeRepository",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListAllowedRepositoriesForGroup",
        "codeartifact:ListDomains",
        "codeartifact:ListPackageGroups",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetFleets",
```

```
        "codebuild:ListFleets",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codedeploy:GetApplication",
        "codedeploy:GetDeployment",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentConfigs",
        "codedeploy:ListDeploymentGroups",
        "codedeploy:ListDeployments",
        "codedeploy:ListTagsForResource",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-profiler:ListTagsForResource",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:ListTagsForResource",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "codepipeline:ListWebhooks",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:ListConnections",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListSyncConfigurations",
        "codestar-connections:ListTagsForResource",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:ListNotificationRules",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
```

```
        "cognito-idp:DescribeTerms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTerms",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "comprehend:DescribeDocumentClassifier",
        "comprehend:DescribeFlywheel",
        "comprehend:DescribeResourcePolicy",
        "comprehend:ListDocumentClassifiers",
        "comprehend:ListFlywheels",
        "comprehend:ListTagsForResource",
        "config:DescribeAggregationAuthorizations",
        "config:DescribeComplianceByConfigRule",
        "config:DescribeConfigRules",
        "config:DescribeConfigurationAggregators",
        "config:DescribeConformancePacks",
        "config:DescribeOrganizationConformancePacks",
        "config:DescribeRemediationConfigurations",
        "config:GetStoredQuery",
        "config:ListStoredQueries",
        "config:ListTagsForResource",
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:ListCampaigns",
        "connect:DescribeAgentStatus",
        "connect:DescribeContactFlow",
        "connect:DescribeContactFlowModule",
        "connect:DescribeContactFlowModuleAlias",
        "connect:DescribeDataTable",
        "connect:DescribeEvaluationForm",
        "connect:DescribeHoursOfOperation",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribeNotification",
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
```

```
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUserHierarchyGroup",
        "connect:DescribeView",
        "connect:DescribeWorkspace",
        "connect:GetTaskTemplate",
        "connect:ListAgentStatuses",
        "connect:ListApprovedOrigins",
        "connect:ListBots",
        "connect:ListContactFlowModuleAliases",
        "connect:ListContactFlowModuleVersions",
        "connect:ListContactFlowModules",
        "connect:ListContactFlowVersions",
        "connect:ListContactFlows",
        "connect:ListDataTableAttributes",
        "connect:ListDataTables",
        "connect:ListEvaluationFormVersions",
        "connect:ListEvaluationForms",
        "connect:ListHoursOfOperationOverrides",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstanceStorageConfigs",
        "connect:ListInstances",
        "connect:ListIntegrationAssociations",
        "connect:ListLambdaFunctions",
        "connect:ListNotifications",
        "connect:ListPredefinedAttributes",
        "connect:ListPrompts",
        "connect:ListQueueEmailAddresses",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileManualAssignmentQueues",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfileFlowModules",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
```

```
        "connect:ListTaskTemplates",
        "connect:ListTrafficDistributionGroups",
        "connect:ListUserHierarchyGroups",
        "connect:ListUserProficiencies",
        "connect:ListUsers",
        "connect:ListViewVersions",
        "connect:ListViews",
        "connect:ListWorkspaceMedia",
        "connect:ListWorkspacePages",
        "connect:ListWorkspaces",
        "connect:SearchWorkspaceAssociations",
        "controltower:GetEnabledBaseline",
        "controltower:GetEnabledControl",
        "controltower:GetLandingZone",
        "controltower:ListEnabledBaselines",
        "controltower:ListEnabledControls",
        "controltower:ListLandingZones",
        "controltower:ListTagsForResource",
        "cur:DescribeReportDefinitions",
        "cur:ListTagsForResource",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationAzureBlob",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxOntap",
        "datasync:DescribeLocationFsxOpenZfs",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
```

```
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "datazone:GetDataSource",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentProfile",
        "datazone:GetGroupProfile",
        "datazone:GetProject",
        "datazone:GetProjectProfile",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListDomains",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjectProfiles",
        "datazone:ListProjects",
        "datazone:ListSubscriptionTargets",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetLicenseEndpoint",
        "deadline:GetLimit",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
```

```
        "deadline:GetQueueFleetAssociation",
        "deadline:GetQueueLimitAssociation",
        "deadline:GetStorageProfile",
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListLicenseEndpoints",
        "deadline:ListLimits",
        "deadline:ListMeteredProducts",
        "deadline:ListMonitors",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListQueueLimitAssociations",
        "deadline:ListQueues",
        "deadline:ListStorageProfiles",
        "deadline:ListTagsForResource",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetMembers",
        "detective:ListGraphs",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "devicefarm:GetDevicePool",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:GetVPCEConfiguration",
        "devicefarm:ListDevicePools",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devicefarm:ListVPCEConfigurations",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListNotificationChannels",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeLags",
        "directconnect:DescribeVirtualInterfaces",
        "dms:DescribeDataMigrations",
        "dms:DescribeReplicationConfigs",
```

```
        "dms:ListDataProviders",
        "dms:ListInstanceProfiles",
        "dms:ListMigrationProjects",
        "dms:ListTagsForResource",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:ListTagsForResource",
        "dsql:GetCluster",
        "dsql:GetClusterPolicy",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeEndpoints",
        "dynamodb:DescribeExport",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeImport",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddressTransfers",
        "ec2:DescribeAddresses",
        "ec2:DescribeAddressesAttribute",
        "ec2:DescribeAggregateIdFormat",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAwsNetworkPerformanceMetricSubscriptions",
        "ec2:DescribeBundleTasks",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeCapacityBlockExtensionHistory",
        "ec2:DescribeCapacityBlockExtensionOfferings",
```

```
        "ec2:DescribeCapacityBlockOfferings",
        "ec2:DescribeCapacityBlockStatus",
        "ec2:DescribeCapacityBlocks",
        "ec2:DescribeCapacityManagerDataExports",
        "ec2:DescribeCapacityReservationBillingRequests",
        "ec2:DescribeCapacityReservationCancellationQuotes",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservationTopology",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeClientVpnAuthorizationRules",
        "ec2:DescribeClientVpnConnections",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeClientVpnRoutes",
        "ec2:DescribeClientVpnTargetNetworks",
        "ec2:DescribeCoipPools",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDeclarativePoliciesReports",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFastLaunchImages",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImageAttribute",
        "ec2:DescribeFpgaImages",
        "ec2:DescribeHostReservationOfferings",
        "ec2:DescribeHostReservations",
        "ec2:DescribeHosts",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeIdFormat",
        "ec2:DescribeIdentityIdFormat",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImageReferences",
        "ec2:DescribeImageUsageReportEntries",
        "ec2:DescribeImageUsageReports",
        "ec2:DescribeImages",
```

```
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeImportSnapshotTasks",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceConnectEndpoints",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstanceEventNotificationAttributes",
        "ec2:DescribeInstanceEventWindows",
        "ec2:DescribeInstanceImageMetadata",
        "ec2:DescribeInstanceSqlHaHistoryStates",
        "ec2:DescribeInstanceSqlHaStates",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTopology",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamByoasn",
        "ec2:DescribeIpamExternalResourceVerificationTokens",
        "ec2:DescribeIpamPolicies",
        "ec2:DescribeIpamPoolAllocations",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpamPrefixListResolverTargets",
        "ec2:DescribeIpamPrefixListResolvers",
        "ec2:DescribeIpamResourceDiscoveries",
        "ec2:DescribeIpamResourceDiscoveryAssociations",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeIpams",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLockedSnapshots",
        "ec2:DescribeMacHosts",
        "ec2:DescribeMacModificationTasks",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
```

```
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeOutpostLags",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribePrincipalIdFormat",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeRegions",
        "ec2:DescribeReplaceRootVolumeTasks",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeReservedInstancesListings",
        "ec2:DescribeReservedInstancesModifications",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteServerEndpoints",
        "ec2:DescribeRouteServerPeers",
        "ec2:DescribeRouteServers",
        "ec2:DescribeRouteTables",
        "ec2:DescribeScheduledInstanceAvailability",
        "ec2:DescribeScheduledInstances",
        "ec2:DescribeSecondaryInterfaces",
        "ec2:DescribeSecondaryNetworks",
        "ec2:DescribeSecondarySubnets",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeServiceLinkVirtualInterfaces",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotDatafeedSubscription",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeStoreImageTasks",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilterRules",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayMeteringPolicies",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTrunkInterfaceAssociations",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstanceLoggingConfigurations",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEncryptionControls",
        "ec2:DescribeVpcEndpointAssociations",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConcentrators",
```

```
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetIpamPrefixListResolverRules",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetRouteServerAssociations",
        "ec2:GetRouteServerPropagations",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayMeteringPolicyEntries",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:DescribeRepositoryCreationTemplates",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:GetRepositoryPolicy",
        "ecr:GetSigningConfiguration",
        "ecr:ListPullTimeUpdateExclusions",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeDaemon",
        "ecs:DescribeDaemonTaskDefinition",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:ListClusters",
        "ecs:ListDaemonTaskDefinitions",
        "ecs:ListDaemons",
```

```
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeCapability",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListCapabilities",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeServerlessCaches",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticbeanstalk:ListTagsForResource",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticloadbalancing:DescribeCapacityReservation",
```

```
        "elasticloadbalancing:DescribeListenerAttributes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTrustStoreRevocations",
        "elasticloadbalancing:DescribeTrustStores",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListStudioSessionMappings",
        "elasticmapreduce:ListStudios",
        "elemental-inference:GetFeed",
        "elemental-inference:ListFeeds",
        "elemental-inference:ListTagsForResource",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeSecurityConfiguration",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListSecurityConfigurations",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetIdNamespace",
        "entityresolution:GetMatchingWorkflow",
        "entityresolution:GetPolicy",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "entityresolution:ListIdNamespaces",
        "entityresolution:ListMatchingWorkflows",
        "entityresolution:ListSchemaMappings",
        "entityresolution:ListTagsForResource",
        "es:GetApplication",
        "es:ListApplications",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
```

```
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetSegment",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "evs:GetEnvironment",
        "evs:ListEnvironments",
        "evs:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:ListExperimentTemplates",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:GetResourceSet",
        "fms:ListPolicies",
        "fms:ListResourceSetResources",
        "fms:ListResourceSets",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "frauddetector:BatchGetVariable",
        "frauddetector:DescribeDetector",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetDetectors",
        "frauddetector:GetEntityTypes",
```

```
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeS3AccessPointAttachments",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeContainerFleet",
        "gamelift:DescribeContainerGroupDefinition",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScalingPolicies",
        "gamelift:DescribeScript",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListContainerFleets",
        "gamelift:ListContainerGroupDefinitions",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "gamelift:ValidateMatchmakingRuleSet",
        "gameliftstreams:GetApplication",
        "gameliftstreams:GetStreamGroup",
        "gameliftstreams:ListApplications",
        "gameliftstreams:ListStreamGroups",
        "gameliftstreams:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeKey",
```

```
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListKeys",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeCrossAccountAttachment",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCrossAccountAttachments",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "glue:DescribeIntegrations",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetCrawler",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetIntegrationResourceProperty",
        "glue:GetJob",
        "glue:GetRegistry",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetUsageProfile",
        "glue:ListCrawlers",
        "glue:ListIntegrationResourceProperties",
        "glue:ListJobs",
        "glue:ListRegistries",
        "glue:ListSchemaVersions",
        "glue:ListSchemas",
        "glue:ListTriggers",
        "glue:ListUsageProfiles",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
```

```
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetDeployment",
        "greengrass:ListComponentVersions",
        "greengrass:ListDeployments",
        "greengrass:ListTagsForResource",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMembers",
        "guardduty:GetThreatEntitySet",
        "guardduty:GetThreatIntelSet",
        "guardduty:GetTrustedEntitySet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "guardduty:ListMembers",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatEntitySets",
        "guardduty:ListThreatIntelSets",
        "guardduty:ListTrustedEntitySets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
```

```
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
```

```
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
        "imagebuilder:ListWorkflowBuildVersions",
        "imagebuilder:ListWorkflows",
        "inspector2:GetCodeSecurityIntegration",
        "inspector2:GetCodeSecurityScanConfiguration",
        "inspector2:ListCisScanConfigurations",
        "inspector2:ListCodeSecurityIntegrations",
        "inspector2:ListCodeSecurityScanConfigurations",
        "inspector2:ListFilters",
        "inspector2:ListTagsForResource",
        "inspector:DescribeAssessmentTargets",
        "inspector:DescribeAssessmentTemplates",
        "inspector:ListAssessmentTargets",
        "inspector:ListAssessmentTemplates",
        "interconnect:GetConnection",
        "interconnect:ListConnections",
        "interconnect:ListTagsForResource",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "invoicing:GetInvoiceUnit",
        "invoicing:ListInvoiceUnits",
        "invoicing:ListTagsForResource",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCertificateProvider",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeEncryptionConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJob",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
```

```
        "iot:DescribeThingType",
        "iot:GetCommand",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetThingShadow",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:GetV2LoggingOptions",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificateProviders",
        "iot:ListCertificates",
        "iot:ListCommands",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPackageVersions",
        "iot:ListPackages",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListThings",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribeLoggingOptions",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
```

```
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetStateTemplate",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListStateTemplates",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeAssetModelCompositeModel",
        "iotsitewise:DescribeAssetModelInterfaceRelationship",
        "iotsitewise:DescribeComputationModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeDataset",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribeGatewayCapabilityConfiguration",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModelCompositeModels",
```

```
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListComputationModels",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListComponents",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListProperties",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetPartnerAccount",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListServiceProfiles",
```

```
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "iotwireless:ListWirelessGateways",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetIngestConfiguration",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetPublicKey",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStorageConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeReplicator",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "WellArchitectedAgentScanningReadOnly2",
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetDirectConnectGatewayAttachment",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworkPrefixListAssociations",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "nimble:GetStudio",
        "nimble:ListStudios",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:ListTagsForResource",
        "notifications:GetEventRule",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications:ListOrganizationalUnits",
        "notifications:ListTagsForResource",
        "nova-act:GetWorkflowDefinition",
        "nova-act:ListWorkflowDefinitions",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListLinks",
```

```
        "oam:ListSinks",
        "oam:ListTagsForResource",
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "odb:GetCloudAutonomousVmCluster",
        "odb:GetCloudExadataInfrastructure",
        "odb:GetCloudVmCluster",
        "odb:GetDbNode",
        "odb:GetOdbNetwork",
        "odb:GetOdbPeeringConnection",
        "odb:ListCloudAutonomousVmClusters",
        "odb:ListCloudExadataInfrastructures",
        "odb:ListCloudVmClusters",
        "odb:ListDbNodes",
        "odb:ListDbServers",
        "odb:ListOdbNetworks",
        "odb:ListOdbPeeringConnections",
        "odb:ListTagsForResource",
        "omics:GetAnnotationStore",
        "omics:GetConfiguration",
        "omics:GetReferenceStore",
        "omics:GetRunGroup",
        "omics:GetS3AccessPolicy",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:GetWorkflowVersion",
        "omics:ListAnnotationStores",
        "omics:ListConfigurations",
        "omics:ListReferenceStores",
        "omics:ListRunGroups",
        "omics:ListSequenceStores",
```

```
        "omics:ListTagsForResource",
        "omics:ListVariantStores",
        "omics:ListWorkflowVersions",
        "omics:ListWorkflows",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "osis:GetPipeline",
        "osis:GetResourcePolicy",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:ListApplicationInstances",
        "panorama:ListPackages",
        "panorama:ListTagsForResource",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:GetResourcePolicy",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
```

```
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListChallengeMetadata",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "profile:GetCalculatedAttributeDefinition",
        "profile:GetDomain",
        "profile:GetDomainObjectType",
        "profile:GetEventStream",
        "profile:GetEventTrigger",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:GetRecommender",
        "profile:GetSegmentDefinition",
        "profile:ListCalculatedAttributeDefinitions",
        "profile:ListDomainObjectTypes",
        "profile:ListDomains",
        "profile:ListEventStreams",
        "profile:ListEventTriggers",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListRecommenders",
        "profile:ListSegmentDefinitions",
        "profile:ListTagsForResource",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetServiceTemplate",
```

```
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentTemplates",
        "proton:ListServiceTemplates",
        "proton:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:GetDataAccessor",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetPolicy",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:ListApplications",
        "qbusiness:ListDataAccessors",
        "qbusiness:ListDataSources",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListTagsForResource",
        "quicksight:DescribeActionConnector",
        "quicksight:DescribeActionConnectorPermissions",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeCustomPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:DescribeTopic",
        "quicksight:DescribeVPCConnection",
```

```
        "quicksight:ListActionConnectors",
        "quicksight:ListAnalyses",
        "quicksight:ListCustomPermissions",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListFolders",
        "quicksight:ListRefreshSchedules",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "quicksight:ListTopics",
        "quicksight:ListVPCConnections",
        "ram:GetPermission",
        "ram:GetResourceShares",
        "ram:ListPermissionVersions",
        "ram:ListPermissions",
        "rbin:GetRule",
        "rbin:ListRules",
        "rbin:ListTagsForResource",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
```

```
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterDbRevisions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:DescribeCollection",
        "rekognition:DescribeProjects",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListCollections",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:GetPolicy",
        "resiliencehub:GetService",
        "resiliencehub:GetSystem",
        "resiliencehub:GetUserJourney",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListAppVersions",
        "resiliencehub:ListApps",
        "resiliencehub:ListAssertions",
        "resiliencehub:ListInputSources",
        "resiliencehub:ListPolicies",
```

```
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListServiceFunctions",
        "resiliencehub:ListServices",
        "resiliencehub:ListSystems",
        "resiliencehub:ListTagsForResource",
        "resiliencehub:ListUserJourneys",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListViews",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTagSyncTask",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "resource-groups:ListTagSyncTasks",
        "robomaker:DescribeFleet",
        "robomaker:DescribeRobot",
        "robomaker:DescribeRobotApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListFleets",
        "robomaker:ListRobotApplications",
        "robomaker:ListRobots",
        "robomaker:ListSimulationApplications",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
```

```
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53-recovery-readiness:ListTagsForResources",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListQueryLoggingConfigs",
        "route53:ListTagsForResource",
        "route53globalresolver:GetAccessSource",
        "route53globalresolver:GetDNSView",
        "route53globalresolver:GetFirewallDomainList",
        "route53globalresolver:GetFirewallRule",
        "route53globalresolver:GetGlobalResolver",
        "route53globalresolver:GetHostedZoneAssociation",
        "route53globalresolver:ListAccessSources",
        "route53globalresolver:ListAccessTokens",
        "route53globalresolver:ListDNSViews",
        "route53globalresolver:ListFirewallDomainLists",
        "route53globalresolver:ListFirewallRules",
        "route53globalresolver:ListGlobalResolvers",
        "route53globalresolver:ListHostedZoneAssociations",
        "route53globalresolver:ListTagsForResource",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
```

```
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListOutpostResolvers",
        "route53resolver:ListResolverConfigs",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver:ListTagsForResource",
        "rtbfabric:GetCertificateAssociation",
        "rtbfabric:GetInboundExternalLink",
        "rtbfabric:GetLink",
        "rtbfabric:GetLinkRoutingRule",
        "rtbfabric:GetOutboundExternalLink",
        "rtbfabric:GetRequesterGateway",
        "rtbfabric:GetResponderGateway",
        "rtbfabric:ListCertificateAssociations",
        "rtbfabric:ListLinkRoutingRules",
        "rtbfabric:ListLinks",
        "rtbfabric:ListRequesterGateways",
        "rtbfabric:ListResponderGateways",
        "rtbfabric:ListTagsForResource",
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetResourcePolicy",
        "rum:ListAppMonitors",
        "rum:ListRumMetricsDestinations",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
```

```
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetObjectAcl",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints",
```

```
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3:ListTagsForResource",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetInventoryConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:GetMetricsConfiguration",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListTagsForResource",
        "s3files:GetAccessPoint",
        "s3files:GetFileSystem",
        "s3files:GetFileSystemPolicy",
        "s3files:GetMountTarget",
        "s3files:GetSynchronizationConfiguration",
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems",
        "s3files:ListMountTargets",
        "s3files:ListTagsForResource",
        "s3tables:GetNamespace",
        "s3tables:GetTable",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketMetricsConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:GetTableMaintenanceConfiguration",
        "s3tables:GetTablePolicy",
        "s3tables:GetTableStorageClass",
        "s3tables:ListNamespaces",
        "s3tables:ListTableBuckets",
        "s3tables:ListTables",
        "s3tables:ListTagsForResource",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:ListIndexes",
        "s3vectors:ListTagsForResource",
```

```
        "s3vectors:ListVectorBuckets",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribePartnerApp",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeUserProfile",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListClusters",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelCards",
```

```
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListPartnerApps",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSpaces",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTags",
        "sagemaker:ListUserProfiles",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemaVersions",
        "schemas:ListSchemas",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "securityagent:BatchGetAgentSpaces",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetTargetDomains",
        "securityagent:GetApplication",
        "securityagent:ListAgentSpaces",
        "securityagent:ListApplications",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentests",
        "securityagent:ListTagsForResource",
        "securityagent:ListTargetDomains",
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetSecurityControls",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeSecurityHubV2",
```

```
        "securityhub:DescribeStandardsControls",
        "securityhub:GetAggregatorV2",
        "securityhub:GetAutomationRuleV2",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetConnectorV2",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:GetInsights",
        "securityhub:ListAggregatorsV2",
        "securityhub:ListAutomationRules",
        "securityhub:ListAutomationRulesV2",
        "securityhub:ListConfigurationPolicies",
        "securityhub:ListConfigurationPolicyAssociations",
        "securityhub:ListConnectorsV2",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:ListFindingAggregators",
        "securityhub:ListOrganizationAdminAccounts",
        "securityhub:ListSecurityControlDefinitions",
        "securityhub:ListTagsForResource",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "servicecatalog:DescribeConstraint",
        "servicecatalog:DescribePortfolio",
        "servicecatalog:DescribePortfolioShares",
        "servicecatalog:DescribeServiceAction",
        "servicecatalog:DescribeTagOption",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAssociatedAttributeGroups",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListConstraintsForPortfolio",
        "servicecatalog:ListPortfolios",
        "servicecatalog:ListPortfoliosForProduct",
        "servicecatalog:ListPrincipalsForPortfolio",
        "servicecatalog:ListResourcesForTagOption",
        "servicecatalog:ListServiceActions",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
```

```
        "servicecatalog:ListTagOptions",
        "servicecatalog:ListTagsForResource",
        "ses:DescribeConfigurationSet",
        "ses:GetAddonInstance",
        "ses:GetAddonSubscription",
        "ses:GetAddressList",
        "ses:GetArchive",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetCustomVerificationEmailTemplate",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailIdentity",
        "ses:GetEmailTemplate",
        "ses:GetIngressPoint",
        "ses:GetMultiRegionEndpoint",
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTenant",
        "ses:GetTrafficPolicy",
        "ses:ListAddonInstances",
        "ses:ListAddonSubscriptions",
        "ses:ListAddressLists",
        "ses:ListArchives",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListCustomVerificationEmailTemplates",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailIdentities",
        "ses:ListEmailTemplates",
        "ses:ListIngressPoints",
        "ses:ListMultiRegionEndpoints",
        "ses:ListRelays",
        "ses:ListRuleSets",
        "ses:ListTagsForResource",
        "ses:ListTemplates",
        "ses:ListTenantResources",
        "ses:ListTenants",
        "ses:ListTrafficPolicies",
        "shield:DescribeDRTAccess",
        "shield:DescribeEmergencyContactSettings",
        "shield:DescribeProtection",
```

```
        "shield:DescribeProtectionGroup",
        "shield:DescribeSubscription",
        "shield:ListProtectionGroups",
        "shield:ListProtections",
        "shield:ListTagsForResource",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "simspaceweaver:DescribeSimulation",
        "simspaceweaver:ListSimulations",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeProtectConfigurations",
        "sms-voice:DescribeSenderIds",
        "sms-voice:GetProtectConfigurationCountryRuleSet",
        "sms-voice:GetResourcePolicy",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "sns:GetDataProtectionPolicy",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:ListQueues",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:GetRotation",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListRotations",
        "ssm-contacts:ListTagsForResource",
        "ssm-guiconnect:GetConnectionRecordingPreferences",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
```

```
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:GetApplication",
        "ssm-sap:ListApplications",
        "ssm-sap:ListTagsForResource",
        "ssm:DescribeAssociation",
        "ssm:DescribeDocument",
        "ssm:DescribeMaintenanceWindowTargets",
        "ssm:DescribeMaintenanceWindowTasks",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetMaintenanceWindow",
        "ssm:GetMaintenanceWindowTask",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso-directory:DescribeGroup",
        "sso-directory:SearchGroups",
        "sso:DescribeApplication",
        "sso:DescribeApplicationAssignment",
        "sso:DescribeInstance",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetManagedApplicationInstance",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:ListAccountAssignments",
        "sso:ListApplicationAssignments",
        "sso:ListApplications",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineAlias",
        "states:ListActivities",
```

```
        "states:ListStateMachineAliases",
        "states:ListStateMachineVersions",
        "states:ListStateMachines",
        "states:ListTagsForResource",
        "sts:GetCallerIdentity",
        "supportapp:GetAccountAlias",
        "supportapp:ListSlackChannelConfigurations",
        "supportapp:ListSlackWorkspaceConfigurations",
        "synthetics:DescribeCanaries",
        "synthetics:GetCanary",
        "synthetics:GetGroup",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "thinclient:GetEnvironment",
        "thinclient:ListEnvironments",
        "thinclient:ListTagsForResource",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeScheduledQuery",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListScheduledQueries",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWebApp",
        "transfer:DescribeWebAppCustomization",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
```

```
        "transfer:ListServers",
        "transfer:ListUsers",
        "transfer:ListWebApps",
        "transfer:ListWorkflows",
        "trustedadvisor:GetRecommendation",
        "trustedadvisor:ListChecks",
        "trustedadvisor:ListRecommendationResources",
        "trustedadvisor:ListRecommendations",
        "trustedadvisor:ListRecommendationsForResource",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyStoreAlias",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyStoreAliases",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "verifiedpermissions:ListTagsForResource",
        "voiceid:DescribeDomain",
        "voiceid:ListDomains",
        "voiceid:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetDomainVerification",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListDomainVerifications",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
```

```
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "wafv2:GetIPSet",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRegexPatternSet",
        "wafv2:GetRuleGroup",
        "wafv2:GetWebACL",
        "wafv2:ListIPSets",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wafv2:ListWebACLs",
        "wisdom:GetAIAgent",
        "wisdom:GetAIGuardrail",
        "wisdom:GetAIPrompt",
        "wisdom:GetAssistant",
        "wisdom:GetAssistantAssociation",
        "wisdom:GetKnowledgeBase",
        "wisdom:GetMessageTemplate",
        "wisdom:GetQuickResponse",
        "wisdom:ListAIAgentVersions",
        "wisdom:ListAIAgents",
        "wisdom:ListAIGuardrailVersions",
        "wisdom:ListAIGuardrails",
        "wisdom:ListAIPromptVersions",
        "wisdom:ListAIPrompts",
        "wisdom:ListAssistantAssociations",
        "wisdom:ListAssistants",
        "wisdom:ListKnowledgeBases",
        "wisdom:ListMessageTemplateVersions",
        "wisdom:ListMessageTemplates",
        "wisdom:ListQuickResponses",
        "workspaces-instances:GetWorkspaceInstance",
        "workspaces-instances:ListTagsForResource",
        "workspaces-instances:ListWorkspaceInstances",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetDataProtectionSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetIpAccessSettings",
```

```
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetSessionLogger",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListDataProtectionSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListIpAccessSettings",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListSessionLoggers",
        "workspaces-web:ListSessions",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspacesPools",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetIndexingRules",
        "xray:GetSamplingRules",
        "xray:GetTraceSegmentDestination",
        "xray:ListResourcePolicies",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "WellArchitectedAgentScanningReadOnly3",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListReplicators",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListTagsForResource",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra-ranking:DescribeRescoreExecutionPlan",
        "kendra-ranking:ListRescoreExecutionPlans",
        "kendra-ranking:ListTagsForResource",
        "kendra:DescribeDataSource",
        "kendra:DescribeFaq",
        "kendra:DescribeIndex",
        "kendra:ListDataSources",
        "kendra:ListFaqs",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForResource",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:DescribeStreamStorageConfiguration",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
```

```
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeLakeFormationIdentityCenterConfiguration",
        "lakeformation:DescribeResource",
        "lakeformation:GetLFTag",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListLFTags",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCapacityProvider",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionScalingConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListCapacityProviders",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListFunctions",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "launchwizard:GetDeployment",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListTagsForResource",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotReplica",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:GetBotAlias",
```

```
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBotReplicas",
        "lex:ListBotVersions",
        "lex:ListBots",
        "lex:ListIntents",
        "lex:ListSlotTypes",
        "lex:ListSlots",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListTagsForResource",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetLoadBalancers",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeDestinations",
        "logs:DescribeIndexPolicies",
```

```
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeResourcePolicies",
        "logs:DescribeSubscriptionFilters",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetIntegration",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:GetScheduledQuery",
        "logs:GetTransformer",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListScheduledQueries",
        "logs:ListSourcesForS3TableIntegration",
        "logs:ListTagsForResource",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListInferenceSchedulers",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetApplication",
        "m2:GetDeployment",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListDeployments",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:GetAllowList",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetMacieSession",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindingsFilters",
        "managedblockchain:GetAccessor",
        "managedblockchain:ListAccessors",
        "mediaconnect:DescribeBridge",
```

```
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeGateway",
        "mediaconnect:GetRouterInput",
        "mediaconnect:GetRouterNetworkInterface",
        "mediaconnect:GetRouterOutput",
        "mediaconnect:ListBridges",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGateways",
        "mediaconnect:ListRouterInputs",
        "mediaconnect:ListRouterNetworkInterfaces",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListTagsForResource",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeCluster",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeNetwork",
        "medialive:DescribeSdiSource",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:ListChannelPlacementGroups",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListClusters",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListMultiplexPrograms",
        "medialive:ListMultiplexes",
        "medialive:ListNetworks",
        "medialive:ListSdiSources",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:DescribeAsset",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:DescribeChannel",
        "mediapackage:DescribeOriginEndpoint",
        "mediapackage:ListChannels",
```

```
        "mediapackage:ListOriginEndpoints",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediatailor:DescribeChannel",
        "mediatailor:DescribeLiveSource",
        "mediatailor:DescribeSourceLocation",
        "mediatailor:DescribeVodSource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "medical-imaging:GetDatastore",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListTagsForResource",
        "memorydb:DescribeACLs",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeMultiRegionClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:ListTemplates",
        "mpa:GetApprovalTeam",
        "mpa:GetIdentitySource",
        "mpa:ListApprovalTeams",
        "mpa:ListIdentitySources",
        "mpa:ListTagsForResource",
        "mq:DescribeBroker",
        "mq:DescribeConfiguration",
        "mq:DescribeSharedResources",
        "mq:ListBrokers",
        "mq:ListConfigurations",
        "mq:ListTags",
        "neptune-graph:GetGraph",
        "neptune-graph:GetGraphSnapshot",
        "neptune-graph:GetPrivateGraphEndpoint",
```

```
        "neptune-graph:ListGraphSnapshots",
        "neptune-graph:ListGraphs",
        "neptune-graph:ListPrivateGraphEndpoints",
        "neptune-graph:ListTagsForResource",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:DescribeVpcEndpointAssociation",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListVpcEndpointAssociations",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSWellArchitectedDiscoveryServiceRolePolicy

Descrição: Permite WellArchitected acessar AWS serviços e recursos relacionados aos WellArchitected recursos em nome dos clientes.

`AWSWellArchitectedDiscoveryServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 26 de abril de 2023, 18:36 UTC
- Hora da edição: 26 de abril de 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeChecks",
        "trustedadvisor:DescribeCheckItems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "resource-groups:ListGroupResources",
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:GetApplication",
        "servicecatalog:CreateAttributeGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
      ],
      "Resource" : [
        "arn:*:servicecatalog:*:*:/applications/*",
        "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:UpdateAttributeGroup",
        "servicecatalog:DeleteAttributeGroup"
      ],
      "Resource" : [
        "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSWellArchitectedOrganizationsServiceRolePolicy

Descrição: Permite Well-Architected acessar organizações em seu nome.

`AWSWellArchitectedOrganizationsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 23 de junho de 2022, 17:15 UTC
- Hora da edição: 25 de julho de 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSWickrFullAccess

Descrição: esta política concede permissões administrativas completas ao serviço Wickr, incluindo às funções administrativas do Wickr sob o Console de gerenciamento da AWS.

`AWSWickrFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSWickrFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de novembro de 2022, 20:36 UTC

- Hora da edição: 27 de novembro de 2022, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWickrFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wickr:*",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSXrayCrossAccountSharingConfiguration

Descrição: fornece recursos para gerenciar links do Observability Access Manager e estabelecer o compartilhamento de X-Ray rastreamentos

`AWSXrayCrossAccountSharingConfiguration` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSXrayCrossAccountSharingConfiguration` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de novembro de 2022, 13:46 UTC
- Hora da edição: 27 de novembro de 2022, 13:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
```

```
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSXRayDaemonWriteAccess

Descrição: permita que o AWS X-Ray Daemon retransmita dados brutos de segmentos de rastreamento para a API do serviço e recupere dados de amostragem (regras, alvos etc.) para serem usados pelo SDK. X-Ray

`AWSXRayDaemonWriteAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSXRayDaemonWriteAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 28 de agosto de 2018, 23:00 UTC
- Hora da edição: 13 de fevereiro de 2024, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSXrayFullAccess

Descrição: política gerenciada de acesso AWS X-Ray total

`AWSXrayFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSXrayFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2016, 18:30 UTC
- Hora da edição: 11 de abril de 2024, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:*"
      ],
      "Resource" : [
```

```
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSXrayReadOnlyAccess

Descrição: política gerenciada somente para AWS X-Ray leitura

`AWSXrayReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSXrayReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2016, 18:27 UTC
- Hora da edição: 14 de fevereiro de 2024, 0:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries",
        "xray:BatchGetTraces",
        "xray:BatchGetTraceSummaryById",
        "xray:GetDistinctTraceGraphs",
        "xray:GetServiceGraph",
        "xray:GetTraceGraph",
        "xray:GetTraceSummaries",
        "xray:GetGroups",
        "xray:GetGroup",
        "xray:ListTagsForResource",
        "xray:ListResourcePolicies",
        "xray:GetTimeSeriesServiceStatistics",
        "xray:GetInsightSummaries",
        "xray:GetInsight",
        "xray:GetInsightEvents",
        "xray:GetInsightImpactGraph"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSXrayWriteOnlyAccess

Descrição: AWS X-Ray escreva somente uma política gerenciada

`AWSXrayWriteOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `AWSXrayWriteOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2016, 18:19 UTC
- Hora da edição: 28 de agosto de 2018, 23:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
```

```
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSZonalAutoshiftPracticeRunSLRPolicy

Descrição: Fornece acesso administrativo para treinos de turnos zonais do ARC e acesso aos status de CloudWatch alarme para monitorar os treinos.

`AWSZonalAutoshiftPracticeRunSLRPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 29 de novembro de 2023, 17:34 UTC
- Horário editado: 30 de junho de 2025, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MonitoringPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "health:DescribeEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoshiftPracticeCheckPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:DescribeInstances",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ZonalShiftManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:CancelZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:UpdateZonalShift"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

AWSZoneGroupAccessManagementServiceRolePolicy

Descrição: fornece acesso somente de leitura às APIs necessárias para oferecer às organizações suporte ao gerenciamento de acesso a grupos de zonas.

`AWSZoneGroupAccessManagementServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 01 de julho de 2025, 19:07 UTC
- Horário editado: 01 de julho de 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZoneGroupAccessManagementServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AwsOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

BatchServiceRolePolicy

Descrição: Fornece acesso ao serviço AWS Batch para gerenciar os recursos necessários, incluindo os recursos do Amazon EC2 e do Amazon ECS.

`BatchServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Hora da criação: 10 de março de 2021, 6:55 UTC
- Horário editado: 05 de agosto de 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBatchPolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:RequestSpotFleet",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
```

```
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "eks:DescribeCluster",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "ecs:DeregisterTaskDefinition",
        "ecs:TagResource",
        "ecs:ListAccountSettings",
        "logs:DescribeLogGroups",
        "iam:GetInstanceProfile",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement2",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement3",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*:log-stream:*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement4",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateOrUpdateTags"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement5",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "ecs.amazonaws.com",
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement6",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "autoscaling.amazonaws.com",
            "ecs.amazonaws.com",
            "ecs-compute.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "AWSBatchPolicyStatement7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CancelSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement9",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteLaunchConfiguration"
      ],
      "Resource" :
 "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement10",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
```

```
        "autoscaling:SetDesiredCapacity",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:SuspendProcesses",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:TerminateInstanceInAutoScalingGroup"
      ],
      "Resource" : "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement11",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteCluster",
        "ecs:DeregisterContainerInstance",
        "ecs:PutClusterCapacityProviders",
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:UpdateCluster"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement12",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask"
      ],
      "Resource" : "arn:aws:ecs:*:*:task-definition/*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement13",
      "Effect" : "Allow",
      "Action" : [
        "ecs:StopTask"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement14",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement15",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*:*:elastic-gpu/*",
        "arn:aws:elastic-inference:*:*:elastic-inference-accelerator/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    },
    {
      "Sid" : "AWSBatchPolicyStatement16",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement17",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateLaunchTemplate",
            "RequestSpotFleet"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement18",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCapacityProvider",
        "ecs:UpdateCapacityProvider",
        "ecs:DeleteCapacityProvider"
      ],
      "Resource" : "arn:aws:ecs:*:*:capacity-provider/AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement19",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:capacity-provider/AWSBatch*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

BedrockAgentCoreFullAccess

Descrição: Fornece acesso total ao Bedrock AgentCore , bem como acesso limitado aos serviços relacionados

`BedrockAgentCoreFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `BedrockAgentCoreFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 16 de julho de 2025, 13:37 UTC
- Horário editado: 03 de setembro de 2026, 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/BedrockAgentCoreFullAccess`

Versão da política

Versão da política: v21 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAgentCoreFullAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:*"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:*"
    },
    {
      "Sid" : "IAMListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "BedrockAgentCorePassRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*BedrockAgentCore*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:bedrock-agentcore*"
    },
    {
      "Sid" : "BedrockAgentCoreKMSReadAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:ListKeys",
        "kms:DescribeKey"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreKMSAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:ListGrants"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "bedrock-agentcore.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreKMSGrantsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
```

```
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "GenerateDataKey"
          ]
        },
        "StringEquals" : {
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:bedrock-agentcore-gateway:arn" : "arn:aws:bedrock-
agentcore:*:*:gateway/*",
          "kms:ViaService" : [
            "bedrock-agentcore.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BedrockAgentCorePolicyKMSGrantsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo"
          ]
        },
        "StringEquals" : {
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:bedrock-agentcore-policy:policy-engine-arn" :
 "arn:aws*:bedrock-agentcore:*:*:policy-engine/*",
```

```
          "kms:ViaService" : [
            "bedrock-agentcore.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::bedrock-agentcore-gateway-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock-agentcore.amazonaws.com",
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreGatewayLambdaAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:*"
      ]
    },
    {
      "Sid" : "BedrockAgentCoreGatewayApiGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/*/stages/*/exports/*"
      ]
    },
    {
      "Sid" : "LoggingAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/bedrock-agentcore/*",
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
    {
      "Sid" : "ObservabilityReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:BatchGet*",
        "application-signals:Get*",
        "application-signals:List*",
        "autoscaling:Describe*",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "oam:ListSinks",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
        "xray:Get*",
        "xray:List*",
        "xray:StartTraceRetrieval",
        "xray:CancelTraceRetrieval",
        "logs:DescribeLogGroups",
        "logs:StartLiveTail",
```

```
        "logs:StopLiveTail"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TransactionSearchXRayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSegmentDestination",
        "xray:UpdateTraceSegmentDestination",
        "xray:GetIndexingRules",
        "xray:UpdateIndexingRule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TransactionSearchLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
    {
      "Sid" : "TransactionSearchLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "TransactionSearchApplicationSignalsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:StartDiscovery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CreateBedrockAgentCoreNetworkServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/network.bedrock-
agentcore.amazonaws.com/AWSServiceRoleForBedrockAgentCoreNetwork",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "network.bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateBedrockAgentCoreGatewayNetworkServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/bedrock-
agentcore.amazonaws.com/AWSServiceRoleForBedrockAgentCoreGatewayNetwork",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateBedrockAgentCoreRuntimeIdentityServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/runtime-identity.bedrock-
agentcore.amazonaws.com/AWSServiceRoleForBedrockAgentCoreRuntimeIdentity",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "runtime-identity.bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateBedrockAgentCoreRuntimeInstancesServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/runtime-instances.bedrock-
agentcore.amazonaws.com/AWSServiceRoleForBedrockAgentCoreRuntimeInstances",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "runtime-instances.bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeS3WriteAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::bedrock-agentcore-runtime-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeS3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeS3ListAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "BedrockAgentCoreRuntimeECRAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeRepositories",
        "ecr:DescribeImages",
        "ecr:ListImages"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationCloudWatchLogCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/bedrock-agentcore/evaluations/*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationCloudWatchLogCustomLogGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentCoreEvaluationCloudWatchLogIndexAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutIndexPolicy",
```

```
        "logs:DescribeIndexPolicies"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws/spans",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationBedrockInvokeAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:inference-profile/*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationLambdaAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:GetFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:*"
    },
    {
      "Sid" : "AgentCoreEvaluationBedrockMantleInference",
      "Effect" : "Allow",
      "Action" : "bedrock-mantle:CreateInference",
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentCoreEvaluationBedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
      "Action" : "bedrock-mantle:CallWithBearerToken",
      "Resource" : "*"
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

BedrockAgentCoreNetworkServiceRolePolicy

Descrição: Permite o acesso a outros recursos AWS de serviço necessários para executar o Amazon Bedrock AgentCore no modo VPC

`BedrockAgentCoreNetworkServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Tempo de criação: 19 de setembro de 2025, 22:04 UTC
- Horário editado: 19 de setembro de 2025, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BedrockAgentCoreNetworkServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateEniInAnySubnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
    },
    {
      "Sid" : "AllowCreateEniWithSecurityGroups",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "AllowCreateEniWithBedrockManagedRequestTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonBedrockAgentCoreManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonBedrockAgentCoreManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowTagEniOnCreate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "AllowManageEniWhenBedrockManaged",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonBedrockAgentCoreManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowGetSecurityGroupsForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetSecurityGroupsForVPC"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "AllowDescribeNetworkingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

BedrockAgentCoreRuntimeIdentityServiceRolePolicy

Descrição: Permite o acesso aos recursos de gerenciamento de identidades e tokens que são necessários para a autenticação e autorização do Amazon Bedrock AgentCore Runtime.

`BedrockAgentCoreRuntimeIdentityServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Tempo de criação: 11 de outubro de 2025, 01:04 UTC
- Horário editado: 11 de outubro de 2025, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BedrockAgentCoreRuntimeIdentityServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Sid" : "AllowWorkloadIdentityAccess",
    "Effect" : "Allow",
    "Action" : [
      "bedrock-agentcore:GetWorkloadAccessToken",
      "bedrock-agentcore:GetWorkloadAccessTokenForJWT",
      "bedrock-agentcore:GetWorkloadAccessTokenForUserId"
    ],
    "Resource" : [
      "arn:aws:bedrock-agentcore:*:*:workload-identity-directory/default",
      "arn:aws:bedrock-agentcore:*:*:workload-identity-directory/default/workload-
identity/*"
    ]
  }
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

BedrockAgentCoreRuntimeInstancesInstanceRolePolicy

Descrição: Política padrão para a função de instância das instâncias gerenciadas pelo Bedrock AgentCore Runtime Instances.

`BedrockAgentCoreRuntimeInstancesInstanceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `BedrockAgentCoreRuntimeInstancesInstanceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 05 de agosto de 2026, 13:27 UTC
- Horário editado: 05 de agosto de 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/BedrockAgentCoreRuntimeInstancesInstanceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowWritingSystemLogs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:PutSystemLogEvents"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:capacity-provider/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

BedrockAgentCoreRuntimeInstancesOperatorRolePolicy

Descrição: Fornece acesso para criar e gerenciar recursos computacionais e associados para instâncias de tempo de execução do Bedrock AgentCore

`BedrockAgentCoreRuntimeInstancesOperatorRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `BedrockAgentCoreRuntimeInstancesOperatorRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 05 de agosto de 2026, 11:27 UTC
- Horário editado: 06 de agosto de 2026, 10:12 UTC
- ARN: `arn:aws:iam::aws:policy/BedrockAgentCoreRuntimeInstancesOperatorRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeComputeResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
```

```
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeNetworkInterfaces",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeEventBridgeRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : "arn:*:events:*:*:rule/agentcore-lifecycle-events-*"
    },
    {
      "Sid" : "CreateVolumeForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/bedrock-agentcore:capacity-provider-id" : "false"
        }
      }
    },
    {
      "Sid" : "AttachVolumeForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateLaunchTemplateForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/bedrock-agentcore:capacity-provider-id" : "false"
        }
      }
    },
    {
      "Sid" : "ModifyLaunchTemplateForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateAutoScalingForManagedInstances",
      "Effect" : "Allow",
```

```
      "Action" : [
        "autoscaling:CreateAutoScalingGroup"
      ],
      "Resource" : "arn:*:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
agentcore-managed-instances-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/bedrock-agentcore:capacity-provider-id" : "false"
        }
      }
    },
    {
      "Sid" : "UpdateAndLaunchAutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:PutLifecycleHook",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:LaunchInstances"
      ],
      "Resource" : "arn:*:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
agentcore-managed-instances-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/bedrock-agentcore:capacity-provider-id" : "false"
        }
      }
    },
    {
      "Sid" : "NetworkingAccessForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateNetworkInterface",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "AmazonAMIsAccessForManagedInstances",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : "amazon"
        }
      }
    },
    {
      "Sid" : "CreateFleetAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*"
      ]
    },
    {
      "Sid" : "LaunchWithManagedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/bedrock-agentcore:capacity-provider-id" : "false"
        }
      }
    },
    {
      "Sid" : "ProvisionEC2InstancesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
```

```
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/bedrock-agentcore:capacity-provider-id" : "false"
        }
      }
    },
    {
      "Sid" : "TagOnCreateManagedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet",
            "CreateLaunchTemplate",
            "RunInstances",
            "CreateVolume",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "TagAfterCreateManagedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "bedrock-agentcore.amazonaws.com"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "bedrock-agentcore:*"
        }
      }
    },
    {
      "Sid" : "AttachNetworkInterfaceToManagedInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventBridgeAccessForManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:*:events:*:*:rule/agentcore-lifecycle-events-*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "bedrock-agentcore.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "ServiceLinkedRoleAccessForAutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/autoscaling.amazonaws.com/
AWSServiceRoleForAutoScaling"
      ]
    },
    {
      "Sid" : "PassRoleToManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/
AmazonBedrockAgentCoreCapacityProviderDefaultInstanceRole*",
        "arn:aws:iam::*:role/service-role/
AmazonBedrockAgentCoreCapacityProviderDefaultInstanceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

Faturamento

Descrição: esta política concede permissões para o gerenciamento de faturamento e custos. Isso inclui visualizar o uso da conta, modificar orçamentos e métodos de pagamento.

`Billing` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `Billing` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de trabalho
- Hora da criação: 10 de novembro de 2016, 17:33 UTC
- Horário editado: 30 de julho de 2026, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/Billing`

Versão da política

Versão da política: v30 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:*Billing",
        "aws-portal:*PaymentMethods",
        "aws-portal:*Usage",
        "billing:CreateBillingView",
```

```
        "billing:DeleteBillingView",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetBillingView",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billing:PutContractInformation",
        "billing:RedeemCredits",
        "billing:GetResourcePolicy",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billing:TagResource",
        "billing:UntagResource",
        "billing:UpdateBillingPreferences",
        "billing:UpdateBillingView",
        "billing:UpdateIAMAccessPreference",
        "budgets:CreateBudgetAction",
        "budgets:DeleteBudgetAction",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "budgets:ExecuteBudgetAction",
        "budgets:ModifyBudget",
        "budgets:UpdateBudgetAction",
        "budgets:ViewBudget",
        "ce:CreateCostCategoryDefinition",
        "ce:CreateNotificationSubscription",
        "ce:CreateReport",
        "ce:DeleteCostCategoryDefinition",
        "ce:DeleteNotificationSubscription",
        "ce:DeleteReport",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostAllocationTags",
        "ce:ListCostCategoryDefinitions",
        "ce:ListCostCategoryResourceAssociations",
        "ce:ListTagsForResource",
        "ce:TagResource",
```

```
        "ce:UpdateCostAllocationTagsStatus",
        "ce:UpdateNotificationSubscription",
        "ce:UpdatePreferences",
        "ce:UpdateReport",
        "ce:UpdateCostCategoryDefinition",
        "ce:UntagResource",
        "ce:StartCostAllocationTagBackfill",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:GetTags",
        "ce:GetDimensionValues",
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "cur:DeleteReportDefinition",
        "cur:DescribeReportDefinitions",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:ModifyReportDefinition",
        "cur:PutClassicReportPreferences",
        "cur:PutReportDefinition",
        "cur:ValidateReportDestination",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:PutFreeTierAlertPreference",
        "invoicing:BatchGetInvoiceProfile",
        "invoicing:CreateInvoiceUnit",
        "invoicing:DeleteInvoiceUnit",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:GetInvoiceUnit",
        "invoicing:GetInvoiceCorrection",
        "invoicing:ListInvoiceSummaries",
        "invoicing:ListInvoiceUnits",
        "invoicing:ListProcurementPortals",
        "invoicing:ListProcurementPortalSuppliers",
        "invoicing:CreateProcurementPortalPreference",
        "invoicing:GetProcurementPortalPreference",
        "invoicing:PutProcurementPortalPreference",
        "invoicing:UpdateProcurementPortalPreferenceStatus",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:DeleteProcurementPortalPreference",
        "invoicing:ListTagsForResource",
        "invoicing:ListInvoiceCorrections",
        "invoicing:StartInvoiceCorrection",
```

```
        "invoicing:PutInvoiceEmailDeliveryPreferences",
        "invoicing:SendProcurementPortalValidation",
        "invoicing:TagResource",
        "invoicing:UntagResource",
        "invoicing:UpdateInvoiceUnit",
        "invoicing:VerifyProcurementPortalValidation",
        "mapcredits:ListQuarterSpend",
        "mapcredits:ListAssociatedPrograms",
        "mapcredits:ListQuarterCredits",
        "payments:CreateFinancingApplication",
        "payments:CreatePaymentInstrument",
        "payments:DeletePaymentInstrument",
        "payments:GetFinancingApplication",
        "payments:GetFinancingLine",
        "payments:GetFinancingLineWithdrawal",
        "payments:GetFinancingOption",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListFinancingApplications",
        "payments:ListFinancingLines",
        "payments:ListFinancingLineWithdrawals",
        "payments:ListPaymentPreferences",
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "payments:ListPaymentInstruments",
        "payments:MakePayment",
        "payments:TagResource",
        "payments:UntagResource",
        "payments:UpdateFinancingApplication",
        "payments:UpdatePaymentInstrument",
        "payments:UpdatePaymentPreferences",
        "pricing:DescribeServices",
        "purchase-orders:AddPurchaseOrder",
        "purchase-orders:DeletePurchaseOrder",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ModifyPurchaseOrders",
        "purchase-orders:TagResource",
        "purchase-orders:UntagResource",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus",
```

```
        "purchase-orders:ViewPurchaseOrders",
        "support:CreateCase",
        "support:AddAttachmentsToSet",
        "sustainability:GetCarbonFootprintSummary",
        "tax:BatchPutTaxRegistration",
        "tax:DeleteTaxRegistration",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "tax:PutTaxInheritance",
        "tax:PutTaxInterview",
        "tax:PutTaxRegistration",
        "tax:UpdateExemptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

BudgetsServiceRolePolicy

Descrição: permite que os Orçamentos verifiquem o acesso às Visualizações de cobrança compartilhadas entre os limites da conta.

`BudgetsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 30 de julho de 2025, 21:07 UTC
- Horário editado: 30 de julho de 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BudgetsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billing:GetBillingViewData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CertificateManagerServiceRolePolicy

Descrição: política de perfil de serviço do Amazon Certificate Manager

`CertificateManagerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 25 de junho de 2020, 17:56 UTC
- Hora da edição: 25 de junho de 2020, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ClientVPNServiceConnectionsRolePolicy

Descrição: Política para permitir que o AWS Client VPN gerencie suas conexões de endpoint do Client VPN.

`ClientVPNServiceConnectionsRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 12 de agosto de 2020, 19:48 UTC
- Hora da edição: 12 de agosto de 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ClientVPNServiceRolePolicy

Descrição: Política para permitir que o AWS Client VPN gerencie seus endpoints do Client VPN.

`ClientVPNServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Horário da criação: 10 de dezembro de 2018, 21:20 UTC
- Hora da edição: 12 de agosto de 2020, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInternetGateways",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAccountAttributes",
        "ds:AuthorizeApplication",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:UnauthorizeApplication",
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "acm:GetCertificate",
        "acm:DescribeCertificate",
        "iam:GetSAMLProvider",
        "lambda:GetFunctionConfiguration"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudFormationStackSetsOrgAdminServiceRolePolicy

Descrição: Função de serviço para CloudFormation StackSets (conta principal da organização)

`CloudFormationStackSetsOrgAdminServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 10 de dezembro de 2019, 0:20 UTC
- Hora da edição: 10 de dezembro de 2019, 0:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsAWSOrganizationsReadAPIs",
      "Effect" : "Allow",
      "Action" : [
        "organizations:List*",
        "organizations:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeRoleInMemberAccounts",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/stacksets-exec-*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudFormationStackSetsOrgMemberServiceRolePolicy

Descrição: Função de serviço para CloudFormation StackSets (conta de membro da organização)

`CloudFormationStackSetsOrgMemberServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 09 de dezembro de 2019, 23:52 UTC
- Horário editado: 22 de julho de 2026, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/stacksets-exec-role-stack-*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/stacksets-exec-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/stacksets-exec-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AdministratorAccess"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudFrontFullAccess

Descrição: Fornece acesso total ao CloudFront console, além da capacidade de listar buckets do Amazon S3 por meio do. Console de gerenciamento da AWS

`CloudFrontFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudFrontFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:39 UTC
- Horário editado: 30 de julho de 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "cffullaccess",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudfront:*",
        "cloudfront-keyvaluestore:*",
        "iam:ListServerCertificates",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "wafv2:CreateWebACL",
        "kinesis:ListStreams",
        "ec2:DescribeInstances",
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:GetIpamPoolCidrs",
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:CreateSubscription",
        "cloudwatch:GetMetricData",
        "freetier:GetAccountPlanState",
        "shield:ListProtections"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "cfrequestcertificate",
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "cloudfront.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "cffdescribestream",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Resource" : "arn:aws:kinesis:*:*:*"
    },
    {
      "Sid" : "cfflistroles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:*"
    },
    {
      "Sid" : "ppmFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:ApprovePaidSubscription",
        "pricingplanmanager:AssociateResourcesToSubscription",
        "pricingplanmanager:CancelSubscription",
        "pricingplanmanager:CancelSubscriptionChange",
        "pricingplanmanager:DisassociateResourcesFromSubscription",
        "pricingplanmanager:GetSubscription",
        "pricingplanmanager:UpdateSubscription"
      ],
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudFrontReadOnlyAccess

Descrição: Fornece acesso às informações CloudFront de configuração de distribuição e distribuições de listas por meio do Console de gerenciamento da AWS.

`CloudFrontReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudFrontReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:39 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudfront:Describe*",
```

```
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "iam:ListServerCertificates",
        "route53:List*",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "ec2:DescribeIpamPools",
        "ec2:GetIpamPoolCidrs",
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:GetSubscription"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudHSMServiceRolePolicy

Descrição: Permite o acesso aos AWS recursos usados ou gerenciados pelo CloudHSM

`CloudHSMServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 06 de novembro de 2017, 19:12 UTC
- Hora da edição: 06 de novembro de 2017, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudSearchFullAccess

Descrição: Fornece acesso total ao serviço de CloudSearch configuração da Amazon.

`CloudSearchFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudSearchFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:39 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudSearchReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao serviço de CloudSearch configuração da Amazon.

`CloudSearchReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudSearchReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:39 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:Describe*",
        "cloudsearch:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudTrailEventContext

Descrição: Essa função vinculada ao serviço permite CloudTrail obter e adicionar tags de recursos aos CloudTrail eventos do proprietário do recurso.

`CloudTrailEventContext` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 15 de maio de 2025, 13:52 UTC
- Horário editado: 15 de maio de 2025, 13:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailEventContext`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailEventContextPermissionForTag",
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeRuleCreation",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : "aws.tag"
        },
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}",
          "events:detail-type" : "Tag Change on Resource",
          "events:ManagedBy" : "context.cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeRuleWrite",
      "Effect" : "Allow",
```

```
      "Action" : [
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*",
      "Condition" : {
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "context.cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeRuleRead",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*"
    },
    {
      "Sid" : "AllowEventBridgeRuleList",
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudTrailServiceRolePolicy

Descrição: Política de permissão para CloudTrail ServiceLinkedRole

`CloudTrailServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 24 de outubro de 2018, 21:21 UTC
- Hora da edição: 27 de novembro de 2023, 1:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AwsOrgsDelegatedAdminAccess",
      "Effect" : "Allow",
      "Action" : "organizations:ListDelegatedAdministrators",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "cloudtrail.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteTableAccess",
      "Effect" : "Allow",
      "Action" : "glue:DeleteTable",
      "Resource" : [
        "arn:*:glue:*:*:catalog",
        "arn:*:glue:*:*:database/aws:cloudtrail",
        "arn:*:glue:*:*:table/aws:cloudtrail/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeregisterResourceAccess",
      "Effect" : "Allow",
```

```
      "Action" : "lakeformation:DeregisterResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatch-CrossAccountAccess

Descrição: Permite CloudWatch assumir CloudWatch-CrossAccountSharing funções em contas remotas em nome da conta atual para exibir dados entre contas e regiões

`CloudWatch-CrossAccountAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 23 de julho de 2019, 9:59 UTC
- Hora da edição: 23 de julho de 2019, 9:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchActionsEC2Access

Descrição: Fornece acesso somente para leitura a CloudWatch alarmes e métricas, bem como aos metadados do EC2. Fornece acesso para parar, encerrar e reinicializar as instâncias do EC2.

`CloudWatchActionsEC2Access` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchActionsEC2Access` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 07 de julho de 2015, 0:00 UTC
- Hora da edição: 07 de julho de 2015, 0:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchAgentAdminPolicy

Descrição: Permissões completas necessárias para usar AmazonCloudWatchAgent.

`CloudWatchAgentAdminPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchAgentAdminPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 07 de março de 2018, 0:52 UTC
- Hora da edição: 5 de fevereiro de 2024, 20:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CWACloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:PutMetricData",
        "ec2:DescribeTags",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWASSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchAgentServerPolicy

Descrição: Permissões necessárias para uso AmazonCloudWatchAgent em servidores

`CloudWatchAgentServerPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchAgentServerPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 07 de março de 2018, 1:06 UTC
- Hora da edição: 6 de fevereiro de 2024, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CWACloudWatchServerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:DescribeVolumes",
        "ec2:DescribeTags",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
```

```
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWASSMServerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchAPIKeyAccess

Descrição: Concede permissões para fazer chamadas CloudWatch usando a autenticação por chave de API.

`CloudWatchAPIKeyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchAPIKeyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Tempo de criação: 08 de maio de 2026, 08:57 UTC
- Horário editado: 04 de junho de 2026, 20:42 UTC

- ARN: `arn:aws:iam::aws:policy/CloudWatchAPIKeyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchMetricsAPIs",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:CallWithBearerToken",
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSDecryptForCMKDatasets",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "cloudwatch.*.amazonaws.com",
          "kms:EncryptionContext:aws:cloudwatch:arn" : "arn:aws:cloudwatch:*:*:dataset/
*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchApplicationInsightsFullAccess

Descrição: Fornece acesso total ao CloudWatch Application Insights e às dependências necessárias.

`CloudWatchApplicationInsightsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchApplicationInsightsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de novembro de 2020, 18:44 UTC
- Hora da edição: 25 de janeiro de 2022, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "sqs:ListQueues",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "autoscaling:DescribeAutoScalingGroups",
        "lambda:ListFunctions",
        "dynamodb:ListTables",
        "s3:ListAllMyBuckets",
        "sns:ListTopics",
        "states:ListStateMachines",
        "apigateway:GET",
        "ecs:ListClusters",
        "ecs:DescribeTaskDefinition",
        "ecs:ListServices",
        "ecs:ListTasks",
        "eks:ListClusters",
        "eks:ListNodegroups",
        "fsx:DescribeFileSystems",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchApplicationInsightsReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao CloudWatch Application Insights.

`CloudWatchApplicationInsightsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchApplicationInsightsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de novembro de 2020, 18:48 UTC
- Hora da edição: 24 de novembro de 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudwatchApplicationInsightsServiceLinkedRolePolicy

Descrição: política de perfil vinculado ao serviço do Cloudwatch Application Insights

`CloudwatchApplicationInsightsServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 01 de dezembro de 2018, 16:22 UTC
- Hora da edição: 25 de julho de 2024, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

Versão da política

Versão da política: v25 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:PutAnomalyDetector",
        "cloudwatch:DeleteAnomalyDetector",
        "cloudwatch:DescribeAnomalyDetectors"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudFormation",
      "Effect" : "Allow",
      "Action" : [
        "cloudFormation:CreateStack",
        "cloudFormation:UpdateStack",
        "cloudFormation:DeleteStack",
        "cloudFormation:DescribeStackResources",
        "cloudFormation:UpdateTerminationProtection"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "CloudFormationStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudFormation:DescribeStacks",
        "cloudFormation:ListStackResources",
        "cloudFormation:ListStacks"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Tag",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ResourceGroups",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationInsightsResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "ElasticLoadBalancing",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-ApplicationInsights-*"
    },
    {
      "Sid" : "SSMAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
```

```
      ]
    },
    {
      "Sid" : "SSMOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:CreateOpsItem",
        "ssm:DescribeOpsItems",
        "ssm:UpdateOpsItem",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMTags",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Sid" : "SSMGetCommandInvocation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMSendCommand",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AWSEC2-CheckPerformanceCounterSets",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AWSEC2-DetectWorkload",
```

```
        "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
      ]
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeNatGateways"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Lambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions",
        "lambda:GetFunctionConfiguration",
        "lambda:ListEventSourceMappings"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EventBridgeManagedRule",
      "Effect" : "Allow",
```

```
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AmazonCloudWatch-ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "XRay",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph",
        "xray:GetTraceSummaries",
        "xray:GetTimeSeriesServiceStatistics",
        "xray:GetTraceGraph"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DynamoDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeTimeToLive"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationAutoscaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "S3",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetMetricsConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "States",
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:DescribeExecution",
        "states:DescribeStateMachine",
        "states:GetExecutionHistory"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "APIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
```

```
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTasks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ECSCluster",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateClusterSettings"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "EKS",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetSubscriptionAttributes",
```

```
        "sns:GetTopicAttributes",
        "sns:GetSMSAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SQS",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsDeleteSubscriptionFilter",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid" : "CloudWatchLogsCreateSubscriptionFilter",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*",
        "arn:aws:logs:*:*:destination:AmazonCloudWatch-ApplicationInsights-
LogIngestionDestination*"
      ]
    },
    {
      "Sid" : "EFS",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFileSystems"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Route53",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHealthCheck",
        "route53:ListHostedZones",
        "route53:ListHealthChecks",
        "route53:ListQueryLoggingConfigs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Route53Resolver",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetFirewallRuleGroupAssociation"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchApplicationSignalsFullAccess

Descrição: Forneça acesso total ao serviço CloudWatch Application Signals e acesso com escopo às dependências necessárias para usar e operar esse serviço.

`CloudWatchApplicationSignalsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchApplicationSignalsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de junho de 2024, 22:50 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsFullAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : "application-signals:*",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSyntheticsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsRumPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rum:BatchCreateRumMetricDefinitions",
        "rum:BatchDeleteRumMetricDefinitions",
        "rum:BatchGetRumMetricDefinitions",
```

```
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:PutRumMetricsDestination",
        "rum:UpdateRumMetricDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayTracePermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:StartTraceRetrieval",
        "xray:ListRetrievedTraces",
        "xray:BatchGetTraces",
        "xray:GetTraceSegmentDestination"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-signals.cloudwatch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsPutMetricAlarmPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricAlarm",
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:SLO-AttainmentGoalAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLO-WarningAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLI-HealthAlarm-*"
      ]
    },
```

```
    {
      "Sid" : "CloudWatchApplicationSignalsCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:cloudwatch-application-signals-*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsReadPermissions",
      "Effect" : "Allow",
      "Action" : "sns:ListTopics",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
```

```
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerCreateIndexPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateIndex"
      ],
      "Resource" : "arn:aws:resource-explorer-2:*:*:index/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMAttachedLinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMListSinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchApplicationSignalsReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao serviço CloudWatch Application Signals e acesso com escopo às dependências necessárias para usar esse serviço

`CloudWatchApplicationSignalsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchApplicationSignalsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 6 de junho de 2024, 20:48 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsReadOnlyAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsReadOnlyAccessPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServiceDependencies",
        "application-signals:ListServiceDependents",
        "application-signals:ListServiceOperations",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource",
        "application-signals:ListServiceStates",
        "application-signals:ListAuditFindings",
        "application-signals:ListGroupingAttributeDefinitions",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListEntityEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSyntheticsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsRumReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayTracePermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:StartTraceRetrieval",
        "xray:ListRetrievedTraces",
```

```
        "xray:BatchGetTraces",
        "xray:GetTraceSegmentDestination"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-signals.cloudwatch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
```

```
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMAttachedLinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMListSinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchApplicationSignalsServiceRolePolicy

Descrição: A política concede permissão à CloudWatch Application Signals para coletar dados de monitoramento e marcação de outros AWS serviços relevantes.

`CloudWatchApplicationSignalsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 09 de novembro de 2023, 18:09 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "XRayPermission",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWLogsPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appsignals/*:*",
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWListMetricsPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWGetMetricDataPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ApplicationSignalsPermission",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:GetServiceLevelObjective"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2AutoScalingPermission",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ResourceExplorerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudTrailServiceLinkedChannelCreationPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-signals/*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchAutomaticDashboardsAccess

Descrição: fornece acesso às CloudWatch APIs que não são usadas para exibir painéis CloudWatch automáticos, incluindo o conteúdo de objetos, como funções do Lambda

`CloudWatchAutomaticDashboardsAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchAutomaticDashboardsAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de julho de 2019, 10:01 UTC
- Horário editado: 07 de agosto de 2026, 10:42 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudfront:GetDistribution",
        "cloudfront:ListDistributions",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
```

```
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "elasticache:DescribeCacheClusters",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListTags",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListQueues",
        "synthetics:DescribeCanariesLastRun",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis*"
      ]
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchCrossAccountSharingConfiguration

Descrição: Fornece recursos para gerenciar links do Observability Access Manager e estabelecer o compartilhamento de CloudWatch recursos

`CloudWatchCrossAccountSharingConfiguration` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchCrossAccountSharingConfiguration` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de novembro de 2022, 14:01 UTC
- Hora da edição: 27 de novembro de 2022, 14:01 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchEventsBuiltInTargetExecutionAccess

Descrição: permite que alvos integrados no Amazon CloudWatch Events realizem ações do EC2 em seu nome.

`CloudWatchEventsBuiltInTargetExecutionAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchEventsBuiltInTargetExecutionAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 14 de janeiro de 2016, 18:35 UTC
- Hora da edição: 14 de janeiro de 2016, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchEventsFullAccess

Descrição: Fornece acesso total aos CloudWatch eventos da Amazon.

`CloudWatchEventsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchEventsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de janeiro de 2016, 18:37 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "schemas.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "SecretsManagerAccessForApiDestinations",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!*"
    },
    {
      "Sid" : "IAMPassRoleForCloudWatchEvents",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS_Events_Invoke_Targets"
    },
    {
      "Sid" : "IAMPassRoleAccessForScheduler",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchEventsInvocationAccess

Descrição: permite que o Amazon CloudWatch Events retransmita eventos para os streams no AWS Kinesis Streams em sua conta.

`CloudWatchEventsInvocationAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchEventsInvocationAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 14 de janeiro de 2016, 18:36 UTC
- Hora da edição: 14 de janeiro de 2016, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsInvocationAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchEventsReadOnlyAccess

Descrição: Fornece acesso somente para leitura aos CloudWatch Eventos da Amazon.

`CloudWatchEventsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchEventsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 14 de janeiro de 2016, 18:27 UTC

- Hora da edição: 01 de dezembro de 2022, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:TestEventPattern",
        "events:DescribeArchive",
        "events:ListArchives",
        "events:DescribeReplay",
        "events:ListReplays",
        "events:DescribeConnection",
        "events:ListConnections",
        "events:DescribeApiDestination",
        "events:ListApiDestinations",
        "events:DescribeEndpoint",
        "events:ListEndpoints",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
```

```
        "schemas:DescribeSchema",
        "schemas:ExportSchema",
        "schemas:GetCodeBindingSource",
        "schemas:GetDiscoveredSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "schemas:SearchSchemas",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchEventsServiceRolePolicy

Descrição: Permite AWS CloudWatch executar ações em seu nome configuradas por meio de alarmes e eventos.

`CloudWatchEventsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 17 de novembro de 2017, 0:42 UTC
- Hora da edição: 17 de novembro de 2017, 0:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:RebootInstances",
        "ec2:StopInstances",
```

```
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchFullAccess

Descrição: Fornece acesso total CloudWatch a.

`CloudWatchFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 27 de novembro de 2022, 13:23 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudwatch:*",
        "logs:*",
        "sns:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchFullAccessV2

Descrição: Fornece acesso total CloudWatch a.

`CloudWatchFullAccessV2` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchFullAccessV2` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de agosto de 2023, 11:32 UTC
- Horário editado: 22 de setembro de 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccessV2`

Versão da política

Versão da política: v17 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "CloudWatchFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:*",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "cloudwatch:*",
        "logs:*",
        "sns:CreateTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks",
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:CreateCentralizationRuleForOrganization",
        "observabilityadmin:UpdateCentralizationRuleForOrganization",
        "observabilityadmin:DeleteCentralizationRuleForOrganization",
        "observabilityadmin:StartTelemetryEvaluation",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:StopTelemetryEvaluation",
        "observabilityadmin:StartTelemetryEvaluationForOrganization",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "observabilityadmin:StopTelemetryEvaluationForOrganization",
        "observabilityadmin:CreateTelemetryRule",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:UpdateTelemetryRule",
        "observabilityadmin:DeleteTelemetryRule",
        "observabilityadmin:CreateTelemetryRuleForOrganization",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:UpdateTelemetryRuleForOrganization",
        "observabilityadmin:DeleteTelemetryRuleForOrganization",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:StartTelemetryEnrichment",
        "observabilityadmin:StopTelemetryEnrichment",
```

```
        "observabilityadmin:TagResource",
        "observabilityadmin:UntagResource",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:CreateTelemetryPipeline",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:UpdateTelemetryPipeline",
        "observabilityadmin:DeleteTelemetryPipeline",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "observabilityadmin:CreateS3TableIntegration",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:DeleteS3TableIntegration",
        "observabilityadmin:CreateDatasetIntegration",
        "observabilityadmin:GetDatasetIntegration",
        "observabilityadmin:ListDatasetIntegrations",
        "observabilityadmin:UpdateDatasetIntegration",
        "observabilityadmin:DeleteDatasetIntegration",
        "rum:*",
        "synthetics:*",
        "xray:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventsServicePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
```

```
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
```

```
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
    {
      "Sid" : "CloudWatchResourceExplorerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchResourceExplorerCreateIndexPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateIndex"
      ],
      "Resource" : "arn:aws:resource-explorer-2:*:*:index/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "logs.amazonaws.com"
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" :
 "arn:aws:observabilityadmin:*:*:s3tableintegration/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "logs.amazonaws.com",
            "telemetry-pipelines.observabilityadmin.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:observabilityadmin:*:*:telemetry-
pipeline/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:CreateTableBucket",
        "s3tables:PutTableBucketEncryption"
      ],
      "Resource" : "arn:aws:s3tables:*:*:bucket/aws-cloudwatch",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "observabilityadmin.amazonaws.com"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3tables:PutTableBucketPolicy"
      ],
      "Resource" : "arn:aws:s3tables:*:*:bucket/aws-cloudwatch"
    },
    {
      "Sid" : "LogAlarmScheduledQueryPassRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "logs.amazonaws.com"
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:logs:*:*:scheduled-query:*"
        }
      }
    },
    {
      "Sid" : "LogAlarmLogLinesPassRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cloudwatch.amazonaws.com"
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:cloudwatch:*:*:alarm:*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchInternetMonitorFullAccess

Descrição: Fornece acesso total às ações para trabalhar com o Amazon CloudWatch Internet Monitor. Também fornece acesso a outros serviços, como Amazon CloudWatch, Amazon EC2, Amazon CloudFront WorkSpaces, Amazon e Elastic Load Balancing, necessários para usar o serviço Internet Monitor para monitorar e armazenar informações sobre o tráfego de aplicativos.

`CloudWatchInternetMonitorFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchInternetMonitorFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 22 de outubro de 2024, 21:02 UTC
- Hora da edição: 22 de outubro de 2024, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FullAccessActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "internetmonitor:CreateMonitor",
        "internetmonitor:DeleteMonitor",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:GetQueryResults",
        "internetmonitor:GetQueryStatus",
        "internetmonitor:Link",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "internetmonitor:StartQuery",
        "internetmonitor:StopQuery",
        "internetmonitor:TagResource",
        "internetmonitor:UntagResource",
        "internetmonitor:UpdateMonitor"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceLinkedRoleActions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/internetmonitor.amazonaws.com/
AWSServiceRoleForInternetMonitor",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "internetmonitor.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "RolePolicyActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/internetmonitor.amazonaws.com/
AWSServiceRoleForInternetMonitor",
      "Condition" : {
        "ArnEquals" : {
```

```
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/aws-service-role/
CloudWatchInternetMonitorServiceRolePolicy"
        }
      }
    },
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudfront:GetDistribution",
        "cloudfront:ListDistributions",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "logs:DescribeLogGroups",
        "logs:GetQueryResults",
        "logs:StartQuery",
        "logs:StopQuery",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchInternetMonitorReadOnlyAccess

Descrição: Fornece acesso somente para leitura às ações para trabalhar com o Amazon CloudWatch Internet Monitor. Também fornece acesso a outros serviços na Amazon CloudWatch, incluindo políticas para recuperar informações sobre CloudWatch métricas e gerenciar consultas de log, que são necessárias para usar o serviço Internet Monitor para monitorar e armazenar informações sobre o tráfego de aplicativos.

`CloudWatchInternetMonitorReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchInternetMonitorReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 12 de novembro de 2024, 23:11 UTC
- Horário editado: 12 de novembro de 2024, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:GetQueryResults",
        "internetmonitor:GetQueryStatus",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
```

```
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "internetmonitor:StartQuery",
        "internetmonitor:StopQuery",
        "logs:DescribeLogGroups",
        "logs:GetQueryResults",
        "logs:StartQuery",
        "logs:StopQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchInternetMonitorServiceRolePolicy

Descrição: Permite que o Internet Monitor acesse o EC2, os espaços de trabalho, CloudFront os recursos e outros serviços necessários em seu nome.

`CloudWatchInternetMonitorServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 27 de novembro de 2022, 17:46 UTC

- Hora da edição: 20 de julho de 2023, 4:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*:log-stream:*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/InternetMonitor"
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchLambdaApplicationSignalsExecutionRolePolicy

Descrição: X-Ray Fornece acesso de gravação a um grupo de registros de sinais de CloudWatch aplicativos.

`CloudWatchLambdaApplicationSignalsExecutionRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchLambdaApplicationSignalsExecutionRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 16 de outubro de 2024, 19:09 UTC
- Hora da edição: 16 de outubro de 2024, 19:09 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaApplicationSignalsExecutionRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsXrayWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogGroupWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchLambdaInsightsExecutionRolePolicy

Descrição: política necessária para a extensão Lambda Insights

`CloudWatchLambdaInsightsExecutionRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchLambdaInsightsExecutionRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 07 de outubro de 2020, 19:27 UTC
- Hora da edição: 07 de outubro de 2020, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda-insights:*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchLogsAPIKeyAccess

Descrição: concede permissões para chamar CloudWatch registros usando a autenticação por chave de API.

`CloudWatchLogsAPIKeyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchLogsAPIKeyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 20 de fevereiro de 2026, 19:42 UTC
- Horário editado: 20 de fevereiro de 2026, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsAPIKeyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LogsAPIs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CallWithBearerToken",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSAPIs",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "logs.*.amazonaws.com"
        },
```

```
        "ArnLike" : {
          "kms:EncryptionContext:aws:logs:arn" : "arn:aws:logs:*:*:log-group:*"
        }
      },
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSDescribeAPIs",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "logs.*.amazonaws.com"
        }
      },
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchLogsCrossAccountSharingConfiguration

Descrição: Fornece recursos para gerenciar links do Observability Access Manager e estabelecer o compartilhamento de recursos de CloudWatch registros

`CloudWatchLogsCrossAccountSharingConfiguration` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchLogsCrossAccountSharingConfiguration` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de novembro de 2022, 13:55 UTC
- Hora da edição: 27 de novembro de 2022, 13:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchLogsFullAccess

Descrição: Fornece acesso total aos CloudWatch registros

`CloudWatchLogsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchLogsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GenerateQueryResultsSummary",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:ListTelemetryPipelines"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchLogsReadOnlyAccess

Descrição: Fornece acesso somente para leitura aos CloudWatch registros

`CloudWatchLogsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchLogsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "cloudwatch:GenerateQuery",
```

```
        "cloudwatch:GenerateQueryResultsSummary",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListTelemetryPipelines"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchNetworkFlowMonitorAgentPublishPolicy

Descrição: você pode usar essa política em perfis do IAM anexados aos recursos de instância do Amazon EC2 e do Amazon EKS para enviar relatórios de telemetria (métricas) para um endpoint do Network Flow Monitor.

`CloudWatchNetworkFlowMonitorAgentPublishPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchNetworkFlowMonitorAgentPublishPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Tempo de criação: 01 de dezembro de 2024, 22:51 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchNetworkFlowMonitorAgentPublishPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "networkflowmonitor:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchNetworkFlowMonitorServiceRolePolicy

Descrição: você não pode se conectar CloudWatchNetworkFlowMonitorServiceRolePolicy às suas entidades do IAM. Essa política está anexada a uma função vinculada ao serviço chamada AWSServiceRoleForNetworkFlowMonitor, que publica os resultados da agregação de telemetria de rede, coletados pelos agentes do Network Flow Monitor, para. CloudWatch Também permite que o serviço use AWS Organizações para obter informações para cenários com várias contas.

`CloudWatchNetworkFlowMonitorServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 01 de dezembro de 2024, 22:36 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorServiceRolePolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NetworkFlowMonitor"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy

Descrição: você não pode se conectar CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy às suas entidades do IAM. Essa política é anexada a uma função vinculada ao serviço chamada AWSServiceRoleForNetworkFlowMonitor _Topology, que gera instantâneos de topologia dos recursos usados pelo Network Flow Monitor em sua conta.

`CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Tempo de criação: 01 de dezembro de 2024, 22:51 UTC
- Horário editado: 01 de setembro de 2026, 01:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TransitGatewayAndVPNStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpnConnections",
        "ec2:GetTransitGatewayRouteTableAssociations",
```

```
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrefixListStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VPCEndpointStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LoadBalancerStatement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroupAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWANStatement",
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:ListCoreNetworks",
        "networkmanager:GetCoreNetwork",
```

```
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:ListAttachments",
        "networkmanager:GetVpcAttachment",
        "networkmanager:GetNetworkRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConfigRecorderCreateDelete",
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForNetworkFlowMonitorTopologyService/*"
      ]
    },
    {
      "Sid" : "ConfigRecorderDescribe",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ConfigRecorderSlrCreation",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "config.amazonaws.com"
```

```
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchNetworkMonitorServiceRolePolicy

Descrição: permite que o CloudWatch Network Monitor acesse e gerencie recursos do EC2 e do VPC, publique dados CloudWatch e acesse outros serviços necessários em seu nome.

`CloudWatchNetworkMonitorServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 21 de dezembro de 2023, 18:53 UTC
- Horário editado: 25 de agosto de 2026, 13:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PublishCw",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NetworkMonitor"
        }
      }
    },
    {
      "Sid" : "DescribeAny",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteModifyEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
```

```
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedByCloudWatchNetworkMonitor" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchOmniAWSIntegrationPolicy

Descrição: Fornece as permissões exigidas pelo CloudWatch Omni para descobrir e ler a topologia AWS de recursos

`CloudWatchOmniAWSIntegrationPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchOmniAWSIntegrationPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Tempo de criação: 22 de setembro de 2026, 04:07 UTC
- Horário editado: 22 de setembro de 2026, 04:07 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOmniAWSIntegrationPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceDiscoveryReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "airflow:List*",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:List*",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetEnvironment",
        "appconfig:List*",
        "application-autoscaling:Describe*",
        "apprunner:Describe*",
        "apprunner:List*",
        "appsync:GetApiAssociation",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetFunction",
```

```
        "appsync:GetGraphqlApi",
        "appsync:GetResolver",
        "appsync:GetSourceApiAssociation",
        "appsync:List*",
        "athena:GetDataCatalog",
        "athena:GetWorkGroup",
        "athena:List*",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAccountSettings",
        "autoscaling:DescribeAdjustmentTypes",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeAutoScalingNotificationTypes",
        "autoscaling:DescribeInstanceRefreshes",
        "autoscaling:DescribeLifecycleHookTypes",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribeLoadBalancerTargetGroups",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeMetricCollectionTypes",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScalingProcessTypes",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeTerminationPolicyTypes",
        "autoscaling:DescribeTrafficSources",
        "autoscaling:DescribeWarmPool",
        "batch:Describe*",
        "batch:List*",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetDataSource",
        "bedrock:GetGuardrail",
        "bedrock:GetKnowledgeBase",
        "bedrock:List*",
        "cloudformation:Describe*",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:List*",
        "cloudfront:Describe*",
```

```
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:List*",
        "cloudtrail:Describe*",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:List*",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Describe*",
        "config:GetAggregateResourceConfig",
        "config:GetResourceConfigHistory",
        "config:GetStoredQuery",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "dax:DescribeClusters",
        "dax:ListTags",
        "directconnect:Describe*",
        "dms:Describe*",
        "dms:List*",
        "dynamodb:Describe*",
        "dynamodb:GetResourcePolicy",
        "dynamodb:List*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAccountVpcEncryptionControl",
        "ec2:DescribeAddressTransfers",
        "ec2:DescribeAddresses",
        "ec2:DescribeAddressesAttribute",
        "ec2:DescribeAggregateIdFormat",
        "ec2:DescribeApplicationStatus",
        "ec2:DescribeApplicationStatusCheckAssociations",
        "ec2:DescribeApplicationStatusChecks",
        "ec2:DescribeAvailabilityZones",
```

```
        "ec2:DescribeAwsNetworkPerformanceMetricSubscriptions",
        "ec2:DescribeBundleTasks",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeCapacityBlockExtensionHistory",
        "ec2:DescribeCapacityBlockExtensionOfferings",
        "ec2:DescribeCapacityBlockOfferings",
        "ec2:DescribeCapacityBlockStatus",
        "ec2:DescribeCapacityBlocks",
        "ec2:DescribeCapacityManagerDataExports",
        "ec2:DescribeCapacityReservationBillingRequests",
        "ec2:DescribeCapacityReservationCancellationQuotes",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservationTopology",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeClientVpnAuthorizationRules",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeClientVpnRoutes",
        "ec2:DescribeClientVpnTargetNetworks",
        "ec2:DescribeCoipPools",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDeclarativePoliciesReports",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFastLaunchImages",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImageAttribute",
        "ec2:DescribeFpgaImages",
        "ec2:DescribeHostReservationOfferings",
        "ec2:DescribeHostReservations",
        "ec2:DescribeHosts",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeIdFormat",
        "ec2:DescribeIdentityIdFormat",
        "ec2:DescribeImageAttribute",
```

```
        "ec2:DescribeImageReferences",
        "ec2:DescribeImageUsageReportEntries",
        "ec2:DescribeImageUsageReports",
        "ec2:DescribeImages",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeImportSnapshotTasks",
        "ec2:DescribeInstanceConnectEndpoints",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstanceEventNotificationAttributes",
        "ec2:DescribeInstanceEventWindows",
        "ec2:DescribeInstanceImageMetadata",
        "ec2:DescribeInstanceSqlHaHistoryStates",
        "ec2:DescribeInstanceSqlHaStates",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTopology",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamByoasn",
        "ec2:DescribeIpamExternalResourceVerificationTokens",
        "ec2:DescribeIpamInternetRegistryAssociations",
        "ec2:DescribeIpamPolicies",
        "ec2:DescribeIpamPoolAllocations",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpamPrefixListResolverTargets",
        "ec2:DescribeIpamPrefixListResolvers",
        "ec2:DescribeIpamResourceDiscoveries",
        "ec2:DescribeIpamResourceDiscoveryAssociations",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeIpams",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLockedSnapshots",
        "ec2:DescribeMacHosts",
        "ec2:DescribeMacModificationTasks",
        "ec2:DescribeManagedPrefixLists",
```

```
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeOutpostLags",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribePrincipalIdFormat",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeRegions",
        "ec2:DescribeReplaceRootVolumeTasks",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeReservedInstancesListings",
        "ec2:DescribeReservedInstancesModifications",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteServerEndpoints",
        "ec2:DescribeRouteServerPeers",
        "ec2:DescribeRouteServers",
        "ec2:DescribeRouteTables",
        "ec2:DescribeScheduledInstanceAvailability",
        "ec2:DescribeScheduledInstances",
        "ec2:DescribeSecondaryInterfaces",
        "ec2:DescribeSecondaryNetworks",
        "ec2:DescribeSecondarySubnets",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeServiceLinkVirtualInterfaces",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotDatafeedSubscription",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeStoreImageTasks",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilterRules",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayMeteringPolicies",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTrunkInterfaceAssociations",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstanceLoggingConfigurations",
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEncryptionControls",
        "ec2:DescribeVpcEndpointAssociations",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConcentrators",
        "ec2:DescribeVpnGateways",
```

```
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ecr:Describe*",
        "ecr:GetRepositoryPolicy",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
        "eks:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:GetResourcePolicy",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "emr-containers:Describe*",
        "emr-containers:List*",
        "emr-serverless:GetApplication",
        "emr-serverless:List*",
        "es:Describe*",
        "es:List*",
        "events:Describe*",
        "events:List*",
        "firehose:Describe*",
        "firehose:List*",
        "fsx:Describe*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetJob",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTrigger",
        "glue:GetWorkflow",
        "glue:List*",
```

```
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAccountAliases",
        "iam:ListAttachedRolePolicies",
        "iam:ListOpenIDConnectProviders",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "kafka:Describe*",
        "kafka:GetClusterPolicy",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kinesis:Describe*",
        "kinesis:GetResourcePolicy",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kinesisvideo:List*",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:ListAliases",
        "kms:ListGrants",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
```

```
        "memorydb:Describe*",
        "memorydb:List*",
        "mq:Describe*",
        "mq:List*",
        "networkmanager:Describe*",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetVpcAttachment",
        "networkmanager:List*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:List*",
        "pipes:Describe*",
        "pipes:List*",
        "ram:GetPermission",
        "ram:GetResourceShares",
        "ram:List*",
        "rds:Describe*",
        "rds:List*",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:List*",
        "resource-explorer-2:Search",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:List*",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:List*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
```

```
        "route53profiles:List*",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:List*",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetEncryptionConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:List*",
        "secretsmanager:Describe*",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:List*",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:List*",
        "ses:GetAccount",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetEmailIdentity",
        "ses:ListConfigurationSets",
        "ses:ListEmailIdentities",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:List*",
        "ssm:Describe*",
```

```
        "ssm:ListAssociationVersions",
        "ssm:ListAssociations",
        "ssm:ListCloudConnectors",
        "ssm:ListCommands",
        "ssm:ListComplianceItems",
        "ssm:ListComplianceSummaries",
        "ssm:ListDocumentMetadataHistory",
        "ssm:ListDocumentVersions",
        "ssm:ListDocuments",
        "ssm:ListInventoryEntries",
        "ssm:ListNodes",
        "ssm:ListNodesSummary",
        "ssm:ListOpsItemEvents",
        "ssm:ListOpsItemRelatedItems",
        "ssm:ListOpsMetadata",
        "ssm:ListResourceComplianceSummaries",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeMapRun",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineAlias",
        "states:DescribeStateMachineForExecution",
        "states:List*",
        "tag:GetResources",
        "timestream:Describe*",
        "timestream:List*",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayReadAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchOmniDomainAccessPolicy

Descrição: Fornece as permissões necessárias para gerenciar o acesso ao domínio CloudWatch Omni.

`CloudWatchOmniDomainAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchOmniDomainAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 22 de setembro de 2026, 01:47 UTC
- Horário editado: 22 de setembro de 2026, 01:47 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOmniDomainAccessPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchOmniDomainAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListSpacesForOrganization",
        "cloudwatch:CreateDomainAccessGrantForOrganization",
        "cloudwatch:GetDomainAccessGrantForOrganization",
        "cloudwatch:ListDomainAccessGrantsForOrganization",
        "cloudwatch:DeleteDomainAccessGrantForOrganization"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "cloudwatch:HasAccessGrant" : "true"
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchOmniModelInferencePolicy

Descrição: Política gerenciada para os clientes anexarem ao CloudWatch Omni para que os recursos do CloudWatch Omni possam fazer chamadas de inferência do modelo Bedrock, como no Agent Playground ou no Evaluations

`CloudWatchOmniModelInferencePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchOmniModelInferencePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 22 de setembro de 2026, 01:47 UTC
- Horário editado: 22 de setembro de 2026, 01:47 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOmniModelInferencePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AgentCoreEvaluationBedrockInvoke",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentCoreEvaluationBedrockMantleInference",
      "Effect" : "Allow",
      "Action" : "bedrock-mantle:CreateInference",
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentCoreEvaluationBedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
      "Action" : "bedrock-mantle:CallWithBearerToken",
      "Resource" : "*"
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchOmniSpaceAccessPolicy

Descrição: Fornece acesso para gerenciar espaços CloudWatch Omni, visualizar aplicativos, telemetria e outros recursos de observabilidade e monitoramento por meio do novo produto Omni CloudWatch

`CloudWatchOmniSpaceAccessPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchOmniSpaceAccessPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 22 de setembro de 2026, 01:47 UTC
- Horário editado: 22 de setembro de 2026, 01:47 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOmniSpaceAccessPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchOmniSpaceAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:UpdateSpace",
        "cloudwatch:GetSpace",
        "cloudwatch:ListSpaces",
        "cloudwatch:GetDomain",
        "cloudwatch:CreateAccessGrant",
        "cloudwatch:GetAccessGrant",
        "cloudwatch:ListAccessGrants",
        "cloudwatch:DeleteAccessGrant",
        "cloudwatch:SearchPrincipals",
        "cloudwatch:StartTelemetryQuerySession",
        "cloudwatch:StopTelemetryQuerySession",
        "cloudwatch:ListTelemetryQuerySessions",
        "cloudwatch:StopTelemetryQuery",
        "cloudwatch:GetTelemetryQueryResults",
        "cloudwatch:GetRecords",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetContextGraph",
        "cloudwatch:CreateAlert",
        "cloudwatch:GetAlert",
        "cloudwatch:UpdateAlert",
        "cloudwatch:DeleteAlert",
        "cloudwatch:ListAlerts",
        "cloudwatch:CreateOmniDashboard",
        "cloudwatch:GetOmniDashboard",
        "cloudwatch:UpdateOmniDashboard",
        "cloudwatch:DeleteOmniDashboard",
        "cloudwatch:ListOmniDashboards",
        "cloudwatch:CreateAccessProfile",
        "cloudwatch:GetAccessProfile",
        "cloudwatch:UpdateAccessProfile",
        "cloudwatch:DeleteAccessProfile",
        "cloudwatch:ListAccessProfiles",
        "cloudwatch:AssumeAccessProfile",
```

```
        "cloudwatch:CreateView",
        "cloudwatch:GetView",
        "cloudwatch:UpdateView",
        "cloudwatch:DeleteView",
        "cloudwatch:ListViews",
        "cloudwatch:GetPreferences",
        "cloudwatch:UpdatePreferences",
        "cloudwatch:CreateOmniThread",
        "cloudwatch:GetOmniThread",
        "cloudwatch:UpdateOmniThread",
        "cloudwatch:ListOmniThreads",
        "cloudwatch:DeleteOmniThread",
        "cloudwatch:StartOmniThreadSession",
        "cloudwatch:SubmitFeedback",
        "cloudwatch:CreateIntegration",
        "cloudwatch:UpdateIntegration",
        "cloudwatch:GetIntegration",
        "cloudwatch:DeleteIntegration",
        "cloudwatch:ListIntegrations",
        "cloudwatch:InvokeIntegration",
        "cloudwatch:GetIntelligenceConfiguration",
        "cloudwatch:PutIntelligenceConfiguration",
        "cloudwatch:TagResource",
        "cloudwatch:UntagResource",
        "cloudwatch:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:HasAccessGrant" : "true"
        }
      }
    },
    {
      "Sid" : "DenyClassicCloudWatchResourceTagging",
      "Effect" : "Deny",
      "Action" : [
        "cloudwatch:TagResource",
        "cloudwatch:UntagResource",
        "cloudwatch:ListTagsForResource"
      ],
      "NotResource" : [
        "arn:aws:cloudwatch:*:*:space/*",
        "arn:aws:cloudwatch:*:*:domain/*",
```

```
        "arn:aws:cloudwatch:*:*:organization-domain/*",
        "arn:aws:cloudwatch:*:*:access-grant/*",
        "arn:aws:cloudwatch:*:*:organization-access-grant/*",
        "arn:aws:cloudwatch:*:*:access-profile/*",
        "arn:aws:cloudwatch:*:*:omni-dashboard/*",
        "arn:aws:cloudwatch:*:*:alert/*",
        "arn:aws:cloudwatch:*:*:view/*",
        "arn:aws:cloudwatch:*:*:integration/*",
        "arn:aws:cloudwatch:*:*:dataset/*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForCloudWatchOmni",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "cloudwatch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ListRolesAndUsers",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers",
        "iam:ListRoles",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIKeyConfigurationUsers",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUserTags",
        "iam:ListServiceSpecificCredentials"
```

```
      ],
      "Resource" : "arn:aws:iam::*:user/omni/OmniIngestionUser-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KmsListKeysForOmni",
      "Effect" : "Allow",
      "Action" : "kms:ListKeys",
      "Resource" : "*"
    },
    {
      "Sid" : "KmsDescribeKeyForOmni",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KmsCryptoOpsForOmniSpaces",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudwatch.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/cw-omni" : "true"
        },
        "StringLike" : {
```

```
          "kms:EncryptionContext:aws:cloudwatch:arn" : "arn:aws:cloudwatch:*:
${aws:PrincipalAccount}:space/*"
        }
      }
    },
    {
      "Sid" : "KmsCryptoOpsForDatasets",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudwatch.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:cloudwatch:arn" : "arn:aws:cloudwatch:*:
${aws:PrincipalAccount}:dataset/*"
        }
      }
    },
    {
      "Sid" : "KmsCryptoOpsForOmniIntelligence",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudwatch.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
```

```
          "aws:ResourceTag/cw-omni" : "true"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:cloudwatch:account" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KmsCryptoOpsForOmniIntelligenceBranchKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudwatch.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/cw-omni" : "true"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws-crypto-ec:aws:cloudwatch:account" :
"${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ConfigServiceLinkedRecorderManagement",
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "config:ConfigurationRecorderServicePrincipal" : [
            "cloudwatch.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "DescribeConfigurationRecorder",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowConfigServiceLinkedRoleCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AgentCoreEvaluator",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:CreateEvaluator",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:UpdateEvaluator",
        "bedrock-agentcore:DeleteEvaluator",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:Evaluate",
        "bedrock-agentcore:TagResource",
        "bedrock-agentcore:UntagResource",
        "bedrock-agentcore:ListTagsForResource"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:evaluator/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentCoreOnlineEvaluationConfig",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:CreateOnlineEvaluationConfig",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:UpdateOnlineEvaluationConfig",
        "bedrock-agentcore:DeleteOnlineEvaluationConfig",
        "bedrock-agentcore:TagResource",
        "bedrock-agentcore:UntagResource",
        "bedrock-agentcore:ListTagsForResource"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:online-evaluation-config/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentCoreEvaluationDatasets",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GetDataset",
        "bedrock-agentcore:ListDatasets",
        "bedrock-agentcore:ListDatasetVersions",
        "bedrock-agentcore:ListDatasetExamples",
        "bedrock-agentcore:CreateDataset",
        "bedrock-agentcore:UpdateDataset",
        "bedrock-agentcore:CreateDatasetVersion",
        "bedrock-agentcore:AddDatasetExamples",
        "bedrock-agentcore:UpdateDatasetExamples",
        "bedrock-agentcore:DeleteDatasetExamples",
        "bedrock-agentcore:DeleteDataset",
        "bedrock-agentcore:TagResource",
        "bedrock-agentcore:UntagResource",
        "bedrock-agentcore:ListTagsForResource"
```

```
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:dataset/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockFoundationModelDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AgentCorePassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "bedrock-agentcore.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AnnotationAndEvalLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/cloudwatch/*",
        "arn:aws:logs:*:*:log-group:/aws/bedrock-agentcore/evaluations/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "OnlineEvalLogGroupDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KmsCryptoOpsForCMKEvaluators",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:bedrock-agentcore:evaluatorArn" :
"arn:aws:bedrock-agentcore:*:${aws:PrincipalAccount}:evaluator/*"
        }
      }
    },
    {
      "Sid" : "CodeEvaluatorLambdaInvoke",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:GetFunction"
```

```
      ],
      "Resource" : "arn:aws:lambda:*:*:function:cloudwatchCodeEvaluator*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ModelProviderKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModelProviderKeyCreation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:cw-omni-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/cw-omni" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ModelProviderKeyManagement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutSecretValue",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:cw-omni-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/cw-omni" : "true"
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchOpenSearchDashboardAccess

Descrição: Essa política fornece ao usuário acesso para visualizar OpenSearch painéis no console do CloudWatch Logs.

`CloudWatchOpenSearchDashboardAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchOpenSearchDashboardAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 01 de dezembro de 2024, 21:06 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchOpenSearchDashboardsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListIntegrations",
        "logs:GetIntegration",
        "logs:DescribeLogGroups",
        "opensearch:ApplicationAccessAll",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsOpensearchReadAPIs",
      "Effect" : "Allow",
      "Action" : [
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "es:ListApplications"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAPIAccessAll",
      "Effect" : "Allow",
      "Action" : [
        "aoss:APIAccessAll"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDQSCollectionPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:GetApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/OpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDQSResourceQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:GetDirectQueryDataSource"
      ],
```

```
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDirectQueryStatusAccess",
      "Effect" : "Allow",
      "Action" : [
        "opensearch:GetDirectQuery"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchOpenSearchDashboardsFullAccess

Descrição: Essa política fornece acesso ao usuário para criar integração OpenSearch para criar, atualizar, excluir ou visualizar painéis no console do CloudWatch Logs.

`CloudWatchOpenSearchDashboardsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchOpenSearchDashboardsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 01 de dezembro de 2024, 21:06 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardsFullAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchOpenSearchDashboardsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListIntegrations",
        "logs:GetIntegration",
        "logs:DeleteIntegration",
        "logs:PutIntegration",
        "logs:DescribeLogGroups",
        "opensearch:ApplicationAccessAll",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsOpensearchReadAPIs",
      "Effect" : "Allow",
      "Action" : [
        "aoss:BatchGetCollection",
```

```
        "aoss:BatchGetLifecyclePolicy",
        "es:ListApplications"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsOpensearchCreateServiceLinkedAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
opensearchservice.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "opensearchservice.amazonaws.com",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsObservabilityCreateServiceLinkedAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
observability.aoss.amazonaws.com/AWSServiceRoleForAmazonOpenSearchServerless",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "observability.aoss.amazonaws.com",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsCollectionRequestAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "aoss:CreateCollection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:RequestTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:CreateApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:RequestTag/OpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "OpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsCollectionResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:DeleteCollection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
```

```
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:UpdateApplication",
        "es:GetApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/OpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsCollectionPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateSecurityPolicy",
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:DeleteSecurityPolicy",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAPIAccessAll",
```

```
      "Effect" : "Allow",
      "Action" : [
        "aoss:APIAccessAll"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsIndexPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:GetAccessPolicy",
        "aoss:CreateLifecyclePolicy",
        "aoss:DeleteLifecyclePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:index" : "cloudwatch-logs-*",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDQSRequestQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:AddDirectQueryDataSource"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:RequestTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsStartDirectQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "opensearch:StartDirectQuery",
        "opensearch:GetDirectQuery"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*"
    },
    {
      "Sid" : "CloudWatchLogsDQSResourceQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:GetDirectQueryDataSource",
        "es:DeleteDirectQueryDataSource"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "directquery.opensearchservice.amazonaws.com",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "CloudWatchLogsAossTagsAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:TagResource"
      ],
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsEsApplicationTagsAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:AddTags"
      ],
      "Resource" : "arn:aws:opensearch:*:*:application/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchIntegration" : [
            "Dashboards"
          ],
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "OpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsEsDataSourceTagsAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:AddTags"
      ],
```

```
      "Resource" : "arn:aws:opensearch:*:*:datasource/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ],
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchReadOnlyAccess

Descrição: Fornece acesso somente para CloudWatch leitura a.

`CloudWatchReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 22 de setembro de 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

Versão da política

Versão da política: v25 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:BatchGet*",
        "application-signals:Get*",
        "application-signals:List*",
        "autoscaling:Describe*",
        "cloudtrail:ListChannels",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:CreateOneTimeDeepLinkCode",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "oam:ListSinks",
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
```

```
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:GetDatasetIntegration",
        "observabilityadmin:ListDatasetIntegrations",
        "sns:Get*",
        "sns:List*",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
        "xray:Get*",
        "xray:List*",
        "xray:StartTraceRetrieval",
        "xray:CancelTraceRetrieval"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchReadOnlyGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchSyntheticsFullAccess

Descrição: Fornece acesso total aos CloudWatch sintéticos.

`CloudWatchSyntheticsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchSyntheticsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário da criação: 25 de novembro de 2019, 17:39 UTC
- Horário editado: 31 de março de 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::cw-syn-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*/exports/swagger",
        "arn:aws:apigateway:*::/apis"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::cw-syn-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::aws-synthetics-library-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "synthetics.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
```

```
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:Synthetics-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogRecord",
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:GetLogGroupFields"
      ],
```

```
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/cwsyn-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunction",
        "lambda:DeleteFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:cwsyn-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetLayerVersion",
        "lambda:PublishLayerVersion",
        "lambda:DeleteLayerVersion"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:layer:cwsyn-*",
        "arn:aws:lambda:*:*:layer:Synthetics:*",
        "arn:aws:lambda:*:*:layer:Synthetics_Selenium:*",
        "arn:aws:lambda:*:*:layer:AWS-CW-Synthetics*:*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "arn:*:sns:*:*:Synthetics-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CloudWatchSyntheticsReadOnlyAccess

Descrição: Fornece acesso somente para leitura a CloudWatch Synthetics.

`CloudWatchSyntheticsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CloudWatchSyntheticsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário da criação: 25 de novembro de 2019, 17:45 UTC
- Hora da edição: 06 de março de 2020, 19:26 UTC

- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ComprehendDataAccessRolePolicy

Descrição: Política para a função de serviço AWS Comprehend, que permite acesso aos recursos do S3 para acesso aos dados

`ComprehendDataAccessRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ComprehendDataAccessRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 06 de março de 2019, 22:28 UTC
- Hora da edição: 06 de março de 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*Comprehend*",
      "arn:aws:s3:::*comprehend*"
    ]
  }
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ComprehendFullAccess

Descrição: fornece acesso total ao Amazon Comprehend.

`ComprehendFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ComprehendFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2017, 18:08 UTC
- Hora da edição: 05 de dezembro de 2017, 1:36 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ComprehendMedicalFullAccess

Descrição: fornece acesso total ao Amazon Comprehend Medical.

`ComprehendMedicalFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ComprehendMedicalFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de novembro de 2018, 17:55 UTC
- Hora da edição: 27 de novembro de 2018, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehendmedical:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ComprehendReadOnly

Descrição: fornece acesso somente leitura ao Amazon Comprehend.

`ComprehendReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ComprehendReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2017, 18:10 UTC
- Hora da edição: 26 de abril de 2022, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectDominantLanguage",
        "comprehend:BatchDetectDominantLanguage",
        "comprehend:DetectEntities",
        "comprehend:BatchDetectEntities",
        "comprehend:DetectKeyPhrases",
        "comprehend:BatchDetectKeyPhrases",
        "comprehend:DetectPiiEntities",
        "comprehend:ContainsPiiEntities",
        "comprehend:DetectSentiment",
        "comprehend:BatchDetectSentiment",
        "comprehend:DetectSyntax",
        "comprehend:BatchDetectSyntax",
        "comprehend:ClassifyDocument",
        "comprehend:DescribeTopicsDetectionJob",
        "comprehend:ListTopicsDetectionJobs",
        "comprehend:DescribeDominantLanguageDetectionJob",
        "comprehend:ListDominantLanguageDetectionJobs",
```

```
        "comprehend:DescribeEntitiesDetectionJob",
        "comprehend:ListEntitiesDetectionJobs",
        "comprehend:DescribeKeyPhrasesDetectionJob",
        "comprehend:ListKeyPhrasesDetectionJobs",
        "comprehend:DescribePiiEntitiesDetectionJob",
        "comprehend:ListPiiEntitiesDetectionJobs",
        "comprehend:DescribeSentimentDetectionJob",
        "comprehend:DescribeTargetedSentimentDetectionJob",
        "comprehend:ListSentimentDetectionJobs",
        "comprehend:ListTargetedSentimentDetectionJobs",
        "comprehend:DescribeDocumentClassifier",
        "comprehend:ListDocumentClassifiers",
        "comprehend:DescribeDocumentClassificationJob",
        "comprehend:ListDocumentClassificationJobs",
        "comprehend:DescribeEntityRecognizer",
        "comprehend:ListEntityRecognizers",
        "comprehend:ListTagsForResource",
        "comprehend:DescribeEndpoint",
        "comprehend:ListEndpoints",
        "comprehend:ListDocumentClassifierSummaries",
        "comprehend:ListEntityRecognizerSummaries",
        "comprehend:DescribeResourcePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ComputeOptimizerAutomationServiceRolePolicy

Descrição: a política ComputeOptimizerAutomationServiceRolePolicy gerenciada é anexada a uma função vinculada ao serviço que permite que o Compute Optimizer execute ações em seu nome.

`ComputeOptimizerAutomationServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 15 de novembro de 2025, 01:19 UTC
- Horário editado: 15 de novembro de 2025, 01:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerAutomationServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "EBSVolumeModification",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/exclude-from-compute-optimizer-automation" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEBSSnapshot",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RollbackEBSVolumeDeletion",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Tag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ComputeOptimizerReadOnlyAccess

Descrição: Fornece acesso somente para ComputeOptimizer leitura a.

`ComputeOptimizerReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ComputeOptimizerReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 07 de março de 2020, 0:11 UTC
- Horário editado: 20 de novembro de 2024, 21:08 UTC
- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "computeOptimizerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetRecommendationSummaries",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetRDSDatabaseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetIdleRecommendations",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:ListServices",
        "ecs:ListClusters",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "lambda:ListFunctions",
        "lambda:ListProvisionedConcurrencyConfigs",
        "cloudwatch:GetMetricData",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "rds:DescribeDBInstances",
```

```
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ComputeOptimizerServiceRolePolicy

Descrição: Permite ligar ComputeOptimizer para AWS os serviços e coletar detalhes da carga de trabalho em seu nome.

`ComputeOptimizerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 3 de dezembro de 2019, 8:45 UTC
- Horário editado: 27 de maio de 2026, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ComputeOptimizerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AutoScalingAccess",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2Access",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElastiCacheAccess",
      "Effect" : "Allow",
      "Action" : [
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeServerlessCaches"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MemoryDBAccess",
      "Effect" : "Allow",
      "Action" : [
        "memorydb:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DocumentDBAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBClusters"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBAccess",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "WorkSpacesAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspacesConnectionStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListEndpoints",
        "sagemaker:DescribeEndpoint"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ConfigConformsServiceRolePolicy

Descrição: política necessária para que o AWSConfig crie pacotes de conformidade

`ConfigConformsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 25 de julho de 2019, 21:38 UTC
- Hora da edição: 12 de janeiro de 2023, 4:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-
conforms.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeRemediationConfigurations",
        "config:DeleteRemediationConfiguration",
        "config:PutRemediationConfigurations"
      ],
      "Resource" : "arn:aws:config:*:*:remediation-configuration/aws-service-
remediation-configuration/config-conforms.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "remediation.config.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetObject",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::awsconfigconforms*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetStackPolicy",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:ValidateTemplate",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/awsconfigconforms-*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Config"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ConsoleFullAccessFromVercel

Descrição: Para uso com contas criadas por meio da integração do Vercel Marketplace com AWS. Fornece acesso para gerenciar todos os recursos dos serviços integrados ao Vercel Marketplace.

`ConsoleFullAccessFromVercel` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ConsoleFullAccessFromVercel` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 11 de dezembro de 2025, 16:49 UTC
- Horário editado: 09 de abril de 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/ConsoleFullAccessFromVercel`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSQL",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dsql:UpdateCluster",
        "dsql:DbConnectAdmin",
        "dsql:DbConnect"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DynamoDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:UpdateTimeToLive",
        "dynamodb:ConditionCheckItem",
        "dynamodb:UntagResource",
        "dynamodb:PutItem",
        "dynamodb:ListTables",
        "dynamodb:DeleteItem",
        "dynamodb:Scan",
        "dynamodb:ListTagsOfResource",
        "dynamodb:Query",
```

```
        "dynamodb:UpdateItem",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:TagResource",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:DescribeLimits",
        "dynamodb:UpdateTable",
        "dynamodb:GetRecords"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Aurora",
      "Effect" : "Allow",
      "Action" : [
        "rds-db:connect",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "rds:RebootDBInstance",
        "rds:DeleteDBInstance",
        "rds:StartDBInstance",
        "rds:ModifyDBInstance",
        "rds:ApplyPendingMaintenanceAction",
        "rds:StartDBCluster",
        "rds:DeleteDBCluster",
        "rds:RebootDBCluster",
        "rds:CreateDBClusterEndpoint",
        "rds:ModifyDBClusterEndpoint",
        "rds:ModifyDBCluster",
        "rds:DeleteDBClusterEndpoint",
        "rds:FailoverDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:ModifyDBClusterParameterGroup",
        "rds:CopyDBClusterParameterGroup",
        "rds:ResetDBClusterParameterGroup",
        "rds:CreateDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:ModifyDBParameterGroup",
        "rds:CopyDBParameterGroup",
        "rds:DeleteDBParameterGroup",
        "rds:CreateDBParameterGroup",
        "rds:DeleteDBClusterAutomatedBackup",
```

```
        "rds:CopyDBClusterSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:CreateDBClusterSnapshot",
        "rds:DeleteDBClusterSnapshot",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AuroraRestricted",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : "aurora-postgresql"
        }
      }
    },
    {
      "Sid" : "OpenSearchServerless",
      "Effect" : "Allow",
      "Action" : [
        "aoss:APIAccessAll",
        "aoss:DashboardsAccessAll",
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:CreateIndex",
        "aoss:DeleteIndex",
        "aoss:GetAccessPolicy",
        "aoss:GetIndex",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListSecurityPolicies",
        "aoss:ListSecurityConfigs",
```

```
        "aoss:ListTagsForResource",
        "aoss:TagResource",
        "aoss:UntagResource",
        "aoss:AddCollectionToCollectionGroup",
        "aoss:UpdateAccessPolicy",
        "aoss:UpdateCollection",
        "aoss:UpdateCollectionGroup",
        "aoss:UpdateIndex",
        "aoss:UpdateSecurityPolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OpenSearchApplications",
      "Effect" : "Allow",
      "Action" : [
        "es:GetApplication",
        "es:UpdateApplication",
        "es:ListApplications",
        "es:GetDefaultApplicationSetting"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Observability",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "ApplicationAutoscalingIntegration",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "dynamodb"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewFreeTierState",
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ConsoleViewOnlyAccessFromVercel

Descrição: Para uso com contas criadas por meio da integração do Vercel Marketplace com AWS. Fornece acesso para visualizar todos os recursos dos serviços integrados ao Vercel Marketplace.

`ConsoleViewOnlyAccessFromVercel` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ConsoleViewOnlyAccessFromVercel` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 11 de dezembro de 2025, 16:49 UTC
- Horário editado: 09 de abril de 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/ConsoleViewOnlyAccessFromVercel`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSQL",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
```

```
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DynamoDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeLimits"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Aurora",
      "Effect" : "Allow",
      "Action" : [
        "rds:Describe*",
        "rds:ListTagsForResource",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OpenSearchServerless",
      "Effect" : "Allow",
      "Action" : [
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:GetAccessPolicy",
        "aoss:GetIndex",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
```

```
        "aoss:ListCollections",
        "aoss:ListSecurityPolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OpenSearchApplications",
      "Effect" : "Allow",
      "Action" : [
        "es:GetApplication",
        "es:ListApplications"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Observability",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewFreeTierState",
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CostOptimizationHubAdminAccess

Descrição: esta política gerenciada fornece acesso de administrador ao Hub de Otimização de Custos.

`CostOptimizationHubAdminAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CostOptimizationHubAdminAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 19 de dezembro de 2023, 0:03 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:UpdateEnrollmentStatus",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:UpdatePreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cost-optimization-hub:ListEfficiencyMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/cost-optimization-hub.bcm.amazonaws.com/
AWSServiceRoleForCostOptimizationHub"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cost-optimization-hub.bcm.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AllowAWSServiceAccessForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CostOptimizationHubReadOnlyAccess

Descrição: esta política gerenciada fornece acesso somente leitura ao Hub de Otimização de Custos.

`CostOptimizationHubReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `CostOptimizationHubReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 13 de dezembro de 2023, 18:04 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cost-optimization-hub:ListEfficiencyMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CostOptimizationHubServiceRolePolicy

Descrição: permite que o Hub de Otimização de Custos recupere informações da organização e colete dados e metadados relacionados à otimização.

`CostOptimizationHubServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 26 de novembro de 2023, 8:03 UTC
- Horário editado: 17 de julho de 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
```

```
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AwsOrgsScopedAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CostExplorerAccess",
      "Effect" : "Allow",
      "Action" : [
        "ce:ListCostAllocationTags",
        "ce:GetCostAndUsage",
        "ce:GetDimensionValues"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

CustomerProfilesServiceLinkedRolePolicy

Descrição: permite que os perfis de clientes do Amazon Connect acessem AWS serviços e recursos em seu nome.

`CustomerProfilesServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 07 de março de 2023, 22:56 UTC
- Horário editado: 05 de março de 2026, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/CustomerProfiles"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/profile.amazonaws.com/
AWSServiceRoleForProfile_*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "connect-campaigns:PutProfileOutboundRequestBatch"
      ],
      "Resource" : [
        "arn:aws:connect-campaigns:*:*:campaign/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "profile:BatchGetProfile",
        "profile:GetRecommender",
        "profile:GetCalculatedAttributeForProfile",
        "profile:GetProfileRecommendations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

DatabaseAdministrator

Descrição: Concede permissões de acesso total aos AWS serviços e ações necessários para instalar e configurar serviços AWS de banco de dados.

`DatabaseAdministrator` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `DatabaseAdministrator` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de trabalho
- Hora da criação: 10 de novembro de 2016, 17:25 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DatabaseAdministrator`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:Describe*",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:Get*",
        "cloudwatch:List*",
```

```
        "cloudwatch:PutMetricAlarm",
        "datapipeline:ActivatePipeline",
        "datapipeline:CreatePipeline",
        "datapipeline:DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:PutPipelineDefinition",
        "datapipeline:QueryObjects",
        "dynamodb:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticache:*",
        "iam:ListRoles",
        "iam:GetRole",
        "kms:ListKeys",
        "lambda:CreateEventSourceMapping",
        "lambda:CreateFunction",
        "lambda:DeleteEventSourceMapping",
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:Create*",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "pi:CreatePerformanceAnalysisReport",
        "pi:DeletePerformanceAnalysisReport",
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetPerformanceAnalysisReport",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
```

```
        "pi:ListAvailableResourceMetrics",
        "pi:ListPerformanceAnalysisReports",
        "pi:ListTagsForResource",
        "pi:TagResource",
        "pi:UntagResource",
        "rds:*",
        "redshift:*",
        "s3:CreateBucket",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Get*",
        "sns:List*",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject*",
        "s3:Get*",
        "s3:List*",
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutBucketWebsite",
        "s3:PutLifecycleConfiguration",
        "s3:PutReplicationConfiguration",
        "s3:PutObject*",
        "s3:Replicate*",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/rds-monitoring-role",
        "arn:aws:iam::*:role/rdbms-lambda-access",
        "arn:aws:iam::*:role/lambda_exec_role",
        "arn:aws:iam::*:role/lambda-dynamodb-*",
        "arn:aws:iam::*:role/lambda-vpc-execution-role",
        "arn:aws:iam::*:role/DataPipelineDefaultRole",
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

DataScientist

Descrição: Concede permissões aos serviços AWS de análise de dados.

`DataScientist` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `DataScientist` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de trabalho
- Hora da criação: 10 de novembro de 2016, 17:28 UTC
- Horário editado: 02 de setembro de 2026, 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DataScientist`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "autoscaling:*",
        "cloudwatch:*",
        "cloudformation:DescribeStackEvents",
        "datapipeline:Describe*",
        "datapipeline:ListPipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:QueryObjects",
        "dynamodb:*",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CancelSpotFleetRequests",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySpotFleetRequest",
        "ec2:RequestSpotInstances",
        "ec2:RequestSpotFleet",
        "elasticfilesystem:*",
        "elasticmapreduce:*",
        "es:*",
        "firehose:*",
        "fsx:DescribeFileSystems",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListRoles",
```

```
        "kinesis:*",
        "kms:List*",
        "lambda:Create*",
        "lambda:Delete*",
        "lambda:Get*",
        "lambda:InvokeFunction",
        "lambda:PublishVersion",
        "lambda:Update*",
        "lambda:List*",
        "machinelearning:*",
        "sdb:*",
        "rds:*",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "redshift:*",
        "s3:CreateBucket",
        "sns:CreateTopic",
        "sns:Get*",
        "sns:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationCreateStackSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Abort*",
        "s3:DeleteObject",
        "s3:Get*",
        "s3:List*",
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketCors",
        "s3:PutBucketLogging",
        "s3:PutBucketNotification",
        "s3:PutBucketTagging",
        "s3:PutObject",
        "s3:Replicate*",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultRole",
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
        "arn:aws:iam::*:role/EMR_DefaultRole",
        "arn:aws:iam::*:role/kinesis-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListUserProfiles",
        "sagemaker:*App",
        "sagemaker:ListApps"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

DAXServiceRolePolicy

Descrição: esta política permite que o DAX crie e gerencie interface de rede, grupo de segurança, sub-rede e VPC em nome do cliente

`DAXServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 05 de março de 2018, 17:51 UTC
- Hora da edição: 05 de março de 2018, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

DBModDiscoveryAndAssessment

Descrição: Permissões de descoberta e avaliação para conector de banco de dados usado na modernização do banco de dados

`DBModDiscoveryAndAssessment` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `DBModDiscoveryAndAssessment` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 25 de março de 2026, 20:27 UTC
- Horário editado: 25 de março de 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/DBModDiscoveryAndAssessment`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInternetGateways",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBSubnetGroups",
        "dms:DescribeEndpoints",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationTasks",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeOrderableReplicationInstances",
        "dms:ListDataProviders",
        "dms:ListInstanceProfiles",
        "dms:ListMigrationProjects",
        "dms:ModifyReplicationSubnetGroup",
        "secretsmanager:ListSecrets",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:ModifyDBSubnetGroup",
      "Resource" : "arn:aws:rds:*:*:subgrp:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:EnableHttpEndpoint",
        "rds:DisableHttpEndpoint",
        "rds-data:ExecuteStatement"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster:*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dms:DescribeTableStatistics",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTaskIndividualAssessments",
        "dms:DescribeApplicableIndividualAssessments"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:task:*",
        "arn:aws:dms:*:*:assessment-run:*",
        "arn:aws:dms:*:*:instance-profile:*",
        "arn:aws:dms:*:*:data-provider:*",
        "arn:aws:dms:*:*:migration-project:*",
        "arn:aws:dms:*:*:rep:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dms:ListMetadataModelAssessments",
        "dms:ListMetadataModelConversions",
        "dms:ListMetadataModelExports",
        "dms:DescribeMetadataModelImports",
        "dms:DescribeConversionConfiguration",
        "dms:DescribeMetadataModelCreations",
        "dms:DescribeMetadataModel",
        "dms:DescribeMetadataModelChildren",
        "dms:GetTargetSelectionRules"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/dms-vpc-role",
        "arn:aws:iam::*:role/dms-cloudwatch-logs-role",
        "arn:aws:iam::*:role/dms-secrets-manager-role",
        "arn:aws:iam::*:role/dms-s3-access-role",
        "arn:aws:iam::*:role/aws-service-role/dms.amazonaws.com/
AWSServiceRoleForDMSServerless"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole",
        "arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:SecretArn" : "arn:aws:secretsmanager:*:
${aws:PrincipalAccount}:secret:*",
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

DBModProvisioningAndMigration

Descrição: Permissões de provisionamento de recursos e migração de dados para o conector de banco de dados usado na modernização do banco de dados

`DBModProvisioningAndMigration` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `DBModProvisioningAndMigration` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 25 de março de 2026, 20:42 UTC
- Horário editado: 25 de março de 2026, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/DBModProvisioningAndMigration`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:UpdateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx-db-modernization-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx-db-modernization-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Project" : "atx-db-modernization",
          "aws:RequestTag/Owner" : "database-connector",
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetBucketVersioning"
      ],
      "Resource" : [
        "arn:aws:s3:::atx-db-modernization-*",
        "arn:aws:s3:::atx-db-modernization-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationSubnetGroup",
        "dms:CreateInstanceProfile",
        "dms:CreateDataProvider",
        "dms:CreateMigrationProject",
        "dms:CreateEndpoint",
        "dms:AddTagsToResource",
        "rds:CreateDBSubnetGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBInstance",
        "rds:AddTagsToResource",
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:subgrp:*",
        "arn:aws:dms:*:*:instance-profile:*",
        "arn:aws:dms:*:*:data-provider:*",
        "arn:aws:dms:*:*:migration-project:*",
        "arn:aws:rds:*:*:subgrp:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:db:*",
        "arn:aws:ec2:*:*:vpc-endpoint:*",
        "arn:aws:dms:*:*:endpoint:*",
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:task:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Project" : "atx-db-modernization",
          "aws:RequestTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dms:ExportMetadataModelAssessment",
        "dms:StartMetadataModelImport",
        "dms:StartMetadataModelConversion",
        "dms:StartMetadataModelExportToTarget",
        "dms:StartMetadataModelExportAsScripts",
```

```
        "dms:StartMetadataModelAssessment",
        "dms:StartMetadataModelCreation",
        "dms:UpdateConversionConfiguration",
        "dms:UpdateMigrationProject",
        "dms:AddTagsToResource",
        "dms:ListTagsForResource",
        "dms:DeleteMigrationProject",
        "dms:DeleteEndpoint",
        "dms:UpdateInstanceProfile",
        "dms:UpdateDataProvider",
        "dms:DeleteInstanceProfile",
        "dms:DeleteDataProvider",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:migration-project:*",
        "arn:aws:dms:*:*:instance-profile:*",
        "arn:aws:dms:*:*:data-provider:*",
        "arn:aws:dms:*:*:endpoint:*",
        "arn:aws:secretsmanager:*:*:secret:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationInstance",
        "dms:DeleteReplicationInstance",
        "dms:ModifyReplicationInstance",
        "dms:RebootReplicationInstance"
      ],
      "Resource" : "arn:aws:dms:*:*:rep:*",
      "Condition" : {
        "StringEquals" : {
          "dms:rep-tag/Project" : "atx-db-modernization",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dms:DeleteReplicationTask",
        "dms:StartReplicationTask",
        "dms:StopReplicationTask",
        "dms:StartReplicationTaskAssessmentRun",
        "dms:CancelReplicationTaskAssessmentRun"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:task:*",
        "arn:aws:dms:*:*:assessment-run:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "dms:task-tag/Project" : "atx-db-modernization",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/dms-vpc-role",
        "arn:aws:iam::*:role/dms-cloudwatch-logs-role",
        "arn:aws:iam::*:role/dms-secrets-manager-role",
        "arn:aws:iam::*:role/dms-s3-access-role",
        "arn:aws:iam::*:role/DMSPremigrationAssessmentS3Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "iam:PassedToService" : [
            "dms.amazonaws.com",
            "dms.*.amazonaws.com",
            "schema-conversion.dms.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

DBModVirtualSource

Descrição: Fornece permissões para o conector de banco de dados usado pelo ATxHelix durante o fluxo de trabalho de modernização do banco de dados offline (DMS-free)

`DBModVirtualSource` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `DBModVirtualSource` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 06 de julho de 2026, 23:12 UTC

- Horário editado: 06 de julho de 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/DBModVirtualSource`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInternetGateways",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBSubnetGroups",
        "secretsmanager:ListSecrets",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:ModifyDBSubnetGroup",
      "Resource" : "arn:aws:rds:*:*:subgrp:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:EnableHttpEndpoint",
        "rds:DisableHttpEndpoint",
        "rds-data:ExecuteStatement"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:SecretArn" : "arn:aws:secretsmanager:*:
${aws:PrincipalAccount}:secret:*",
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:UpdateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx-db-modernization-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:atx-db-modernization-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Project" : "atx-db-modernization",
          "aws:RequestTag/Owner" : "database-connector",
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetBucketVersioning"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::atx-db-modernization-*",
        "arn:aws:s3:::atx-db-modernization-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBSubnetGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBInstance",
        "rds:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:subgrp:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:db:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Project" : "atx-db-modernization",
          "aws:RequestTag/Owner" : "database-connector",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/Project" : "atx-db-modernization",
          "aws:ResourceTag/Owner" : "database-connector"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

DeclarativePoliciesEC2Report

Descrição: fornece acesso às APIs somente para leitura necessárias para executar o relatório de status da conta das políticas declarativas do EC2.

`DeclarativePoliciesEC2Report` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 30 de novembro de 2024, 13:21 UTC
- Horário editado: 03 de julho de 2026, 10:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DeclarativePoliciesEC2Report`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeclarativePoliciesEC2Report",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:GetInstanceMetadataDefaults",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetAllowedImagesSettings",
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeAccountVpcEncryptionControl"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

Descrição: Permissões necessárias para oferecer suporte ao Amazon CloudWatch Contributor Insights for Amazon DynamoDB.

`DynamoDBCloudWatchContributorInsightsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 15 de novembro de 2019, 21:13 UTC
- Hora da edição: 15 de novembro de 2019, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DeleteInsightRules",
        "cloudwatch:PutInsightRule"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Action" : [
        "cloudwatch:DescribeInsightRules"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

DynamoDBGlobalTableSettingsManagementServiceRolePolicy

Descrição: permissões exigidas pelo DynamoDB para gerenciar as configurações globais de réplica de tabelas.

`DynamoDBGlobalTableSettingsManagementServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 15 de outubro de 2025, 17:34 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBGlobalTableSettingsManagementServiceRolePolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBActionsNeededToReplicateSettings",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget"
      ],
```

```
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*",
        "arn:aws:autoscaling:*:*:scalingPolicy:*:resource/dynamodb/table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : [
            "dynamodb"
          ]
        }
      }
    },
    {
      "Sid" : "DynamoDBReplicationServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

DynamoDBKinesisReplicationServiceRolePolicy

Descrição: Forneça acesso ao AWS DynamoDB ao KinesisDataStreams

`DynamoDBKinesisReplicationServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 12 de novembro de 2020, 0:43 UTC
- Hora da edição: 12 de novembro de 2020, 0:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "kinesis.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

DynamoDBReplicationServiceRolePolicy

Descrição: permissões exigidas pelo DynamoDB para replicação de dados entre regiões

`DynamoDBReplicationServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 09 de novembro de 2017, 23:55 UTC
- Hora da edição: 8 de janeiro de 2024, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBActionsNeededForSteadyStateReplication",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteItem",
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "dynamodb:Scan",
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:UpdateTimeToLive",
        "dynamodb:DescribeLimits",
        "dynamodb:GetResourcePolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DescribeScalingPolicies",
        "account:ListRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBReplicationServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

EC2ApplicationStatusChecksServiceRolePolicy

Descrição: Permite que o EC2 descubra e gerencie recursos relacionados às verificações de status de aplicativos do EC2

`EC2ApplicationStatusChecksServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 27 de abril de 2026, 23:42 UTC
- Horário editado: 15 de julho de 2026, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2ApplicationStatusChecksServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : [
            "ec2.application-status-checks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Usage"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

EC2FastLaunchFullAccess

Descrição: esta política concede total acesso às ações e às ações do EC2 Fast Launch.

`EC2FastLaunchFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `EC2FastLaunchFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 13 de maio de 2024, 22:45 UTC
- Horário editado: 04 de agosto de 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/EC2FastLaunchFullAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2FastLaunch",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch",
        "ec2:DisableFastLaunch",
        "ec2:DescribeFastLaunchImages"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2CreateVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpc"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ModifyDeleteVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpc",
        "ec2:CreateSubnet",
        "ec2:ModifyVpcAttribute",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2CreateSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
```

```
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ManageSecurityGroupEgress",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormation",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:RollbackStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateTerminationProtection",
```

```
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/EC2FastLaunch*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/EC2FastLaunch*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : "CreateStack"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2LaunchTemplateModify",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyLaunchTemplate",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
```

```
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2LaunchInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Sid" : "EC2LaunchInstanceWithVolAndInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "EC2Tags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*",
```

```
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Sid" : "EC2ManageTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2fastlaunch.amazonaws.com/
AWSServiceRoleForEC2FastLaunch",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMSLRPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
```

```
        "arn:aws:iam::*:instance-profile/*",
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

EC2FastLaunchServiceRolePolicy

Descrição: a política concede ao ec2fastlaunch a preparação e o gerenciamento de snapshots pré-provisionados na conta do cliente e a publicação de métricas relacionadas.

`EC2FastLaunchServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 10 de janeiro de 2022, 13:08 UTC

- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowRunInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Sid" : "AllowRunInstancesOnFastLaunchCreatedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
```

```
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStopAndTerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateTaggedSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "StringLike" : {
          "aws:RequestTag/CreatedByLaunchTemplateVersion" : "*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "CreatedByLaunchTemplateName",
            "CreatedByLaunchTemplateId"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCreateLaunchTemplate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSnapshot",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDeleteSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowDeleteVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
```

```
      }
    },
    {
      "Sid" : "AllowDeleteNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeVolumes",
        "ec2:DescribeNetworkInterfaces",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/EC2"
```

```
        }
      }
    },
    {
      "Sid" : "AllowEventsRuleMutations",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:PutRule",
        "events:PutTargets"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ec2fastlaunch.amazonaws.com"
        }
      },
      "Resource" : [
        "arn:aws:events:*:*:rule/FastLaunch*"
      ]
    },
    {
      "Sid" : "AllowEventsRuleNonMutations",
      "Effect" : "Allow",
      "Action" : [
        "events:ListTargetsByRule",
        "events:DescribeRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/FastLaunch*"
      ]
    },
    {
      "Sid" : "AllowKMSActions",
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDeleteFastLaunchLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

EC2FleetTimeShiftableServiceRolePolicy

Descrição: política que concede permissões ao EC2 Fleet para iniciar instâncias no futuro.

`EC2FleetTimeShiftableServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 23 de dezembro de 2019, 19:47 UTC
- Hora da edição: 23 de dezembro de 2019, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstances",
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2:fleet-id" : "*"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

Ec2ImageBuilderCrossAccountDistributionAccess

Descrição: permissões necessárias pelo EC2 Image Builder para realizar uma distribuição entre contas.

`Ec2ImageBuilderCrossAccountDistributionAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `Ec2ImageBuilderCrossAccountDistributionAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada

- Hora da criação: 30 de setembro de 2020, 19:22 UTC
- Hora da edição: 30 de setembro de 2020, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*::image/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:CopyImage",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

EC2ImageBuilderExecutionPolicy

Descrição: Concede permissões que permitem ao EC2 Image Builder chamar AWS serviços em seu nome

`EC2ImageBuilderExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `EC2ImageBuilderExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 04 de junho de 2026, 17:12 UTC
- Horário editado: 08 de julho de 2026, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/EC2ImageBuilderExecutionPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Sid" : "RunInstancesWithEC2ImageBuilderRequestTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
```

```
            "ec2.amazonaws.com.cn",
            "vmie.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EC2InstanceStateChangePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CopyImage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2CreateImagePermissionsForImage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2CreateImagePermissionsForInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2DeregisterImagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2RegisterImagePermissionsForImage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2RegisterImagePermissionsForSnapshot",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2ModifyImageAttributePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2SnapshotAttributeModificationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ],
          "ec2:CreateAction" : [
            "CreateImage",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "CreateCustomerTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:export-image-task/*"
      ]
    },
    {
      "Sid" : "CreateEC2ImageBuilderTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Sid" : "AttachImageWatermarkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachImageWatermark"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "UpdateCustomerLicensePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource"
      ],
      "Resource" : [
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Sid" : "PublishNotificationToCustomerSNSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SystemsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListInventoryEntries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SystemsManagerPermissionsForAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
```

```
      "Sid" : "SystemsManagerPermissionsForInstance",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceAssociationsStatus"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "SendCommandDocumentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ssm:*:*:document/AWSEC2-RunSysprep"
      ]
    },
    {
      "Sid" : "SendCommandEC2ImageBuilderInstancePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "InventoryCollectionAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*",
```

```
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory"
      ]
    },
    {
      "Sid" : "InventoryCollectionInstancePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "InventoryCollectionTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "DeleteInventoryCollectionAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
```

```
      "Sid" : "EC2KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EC2KMSDescribeKeyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EC2KMSGrantKeyPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountAssumeRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/EC2ImageBuilderDistributionCrossAccountRole"
      ]
    },
    {
      "Sid" : "CloudWatchLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
      ]
    },
    {
      "Sid" : "LaunchTemplatePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExportImageBuilderImagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "CreateExportImageTaskPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:export-image-task/*"
      ]
    },
    {
      "Sid" : "CancelExportImageTaskPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelExportTask"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:export-image-task/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
```

```
        }
      }
    },
    {
      "Sid" : "CreateSLRForOtherServicesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ssm.amazonaws.com",
            "ec2fastlaunch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EnableFastLaunchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "ListInspectorFindingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:ListCoverage",
        "inspector2:ListFindings"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CreateECRImageForInspectorScanningPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/image-builder-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "DeleteECRImageForInspectorScanningPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchDeleteImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/image-builder-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EventBridgePermissionsForInspectorScanning",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
```

```
        "arn:aws:events:*:*:rule/ImageBuilder-*"
      ]
    },
    {
      "Sid" : "ParameterStorePermissionsForImageBuilderParameters",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/imagebuilder/*"
      ]
    },
    {
      "Sid" : "ParameterStorePermissionsForServiceManagedParameters",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*::parameter/aws/service/*"
      ]
    },
    {
      "Sid" : "StartImagePipelineExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:StartImagePipelineExecution",
        "imagebuilder:TagResource"
      ],
      "Resource" : [
        "arn:aws:imagebuilder:*:*:image-pipeline/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

EC2ImageBuilderLifecycleExecutionPolicy

Descrição: a EC2ImageBuilderLifecycleExecutionPolicy política concede permissões ao Image Builder para realizar ações como descontinuar ou excluir recursos de imagem do Image Builder e seus recursos subjacentes (AMIs, instantâneos) para dar suporte a regras automatizadas para tarefas de gerenciamento do ciclo de vida de imagens.

`EC2ImageBuilderLifecycleExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `EC2ImageBuilderLifecycleExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 16 de novembro de 2023, 23:23 UTC
- Hora da edição: 16 de novembro de 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImage",
        "ec2:DeregisterImage",
        "ec2:EnableImageDeprecation",
        "ec2:DescribeImageAttribute",
        "ec2:DisableImage",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2TagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
```

```
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeprecatedBy" : "EC2 Image Builder",
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "DeprecatedBy"
        }
      }
    },
    {
      "Sid" : "ECRImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchDeleteImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "ecr:ResourceTag/LifecycleExecutionAccess" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "ImageBuilderEC2TagServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "tag:GetResources",
        "imagebuilder:DeleteImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

EC2InstanceConnect

Descrição: permite que os clientes chamem o EC2 Instance Connect para publicar chaves efêmeras em suas instâncias do EC2 e se conectem via ssh ou pela CLI do EC2 Instance Connect.

`EC2InstanceConnect` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `EC2InstanceConnect` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de junho de 2019, 18:53 UTC
- Hora da edição: 27 de junho de 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

Ec2InstanceConnectEndpoint

Descrição: política de endpoint do EC2 Instance Connect para gerenciar endpoints do EC2 Instance Connect criados pelo cliente

`Ec2InstanceConnectEndpoint` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 24 de janeiro de 2023, 20:19 UTC
- Horário editado: 31 de julho de 2025, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "InstanceConnectEndpointId"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "InstanceConnectEndpointId"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
```

```
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:ModifyNetworkInterfaceAttribute",
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

EC2InstanceProfileForImageBuilder

Descrição: perfil de instância do EC2 para o serviço Image Builder.

`EC2InstanceProfileForImageBuilder` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `EC2InstanceProfileForImageBuilder` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de dezembro de 2019, 19:08 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot",
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*.ISO",
        "arn:aws:s3:::*/*.iso",
```

```
        "arn:aws:s3:::*/*.Iso"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetMarketplaceResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
          "aws:CalledVia" : [
            "imagebuilder.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::ec2imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
```

```
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

EC2InstanceProfileForImageBuilderECRContainerBuilds

Descrição: perfil de instância do EC2 para criar imagens de contêiner com o EC2 Image Builder. Essa política concede ao usuário amplas permissões para fazer upload de imagens do ECR.

`EC2InstanceProfileForImageBuilderECRContainerBuilds` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `EC2InstanceProfileForImageBuilderECRContainerBuilds` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de dezembro de 2020, 19:48 UTC
- Hora da edição: 11 de dezembro de 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
          "aws:CalledVia" : [
            "imagebuilder.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::ec2imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ECRReplicationServiceRolePolicy

Descrição: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pela replicação do ECR

`ECRReplicationServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Hora da criação: 04 de dezembro de 2020, 22:11 UTC
- Hora da edição: 04 de dezembro de 2020, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ECRTemplateServiceRolePolicy

Descrição: permite que ações sejam executadas ao usar modelos de criação de repositórios AWS ECR

`ECRTemplateServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 19 de junho de 2024, 23:11 UTC
- Hora da edição: 19 de junho de 2024, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRTemplateServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateRepositoryWithTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ElastiCacheServiceRolePolicy

Descrição: Essa política permite ElastiCache gerenciar AWS recursos em seu nome conforme necessário para gerenciar seu cache.

`ElastiCacheServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 07 de dezembro de 2017, 17:50 UTC
- Hora da edição: 28 de novembro de 2023, 3:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "cloudwatch:PutMetricData",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDeleteVPCEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
        }
      }
    },
    {
      "Sid" : "TagVPCEndpointsOnCreation",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ElasticLoadBalancingFullAccess

Descrição: Fornece acesso total à Amazon ElasticLoadBalancing e acesso limitado a outros serviços necessários para fornecer ElasticLoadBalancing recursos.

`ElasticLoadBalancingFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ElasticLoadBalancingFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 20 de setembro de 2018, 20:42 UTC
- Horário editado: 23 de fevereiro de 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
```

```
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeAvailabilityZones",
        "cognito-idp:DescribeUserPoolClient"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "arc-zonal-shift:*",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ElasticLoadBalancingReadOnly

Descrição: Fornece acesso somente para leitura à Amazon ElasticLoadBalancing e aos serviços dependentes

`ElasticLoadBalancingReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ElasticLoadBalancingReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 20 de setembro de 2018, 20:17 UTC
- Hora da edição: 26 de novembro de 2023, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Statement2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Statement3",
      "Effect" : "Allow",
      "Action" : "arc-zonal-shift:GetManagedResource",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    },
    {
      "Sid" : "Statement4",
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ElementalActivationsDownloadSoftwareAccess

Descrição: acesso para visualizar ativos adquiridos e baixar software relacionado e arquivos kickstart

`ElementalActivationsDownloadSoftwareAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ElementalActivationsDownloadSoftwareAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 08 de setembro de 2020, 17:26 UTC
- Hora da edição: 08 de setembro de 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:Download*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ElementalActivationsFullAccess

Descrição: acesso total para visualizar e agir sobre os ativos adquiridos de dispositivos e software do Elemental

`ElementalActivationsFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ElementalActivationsFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 04 de junho de 2020, 21:00 UTC
- Hora da edição: 04 de junho de 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ElementalActivationsGenerateLicenses

Descrição: acesso para visualizar ativos adquiridos e gerar licenças de software para ativações pendentes

`ElementalActivationsGenerateLicenses` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ElementalActivationsGenerateLicenses` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de agosto de 2020, 18:28 UTC
- Hora da edição: 28 de agosto de 2020, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ElementalActivationsReadOnlyAccess

Descrição: Read-only acesso à lista detalhada de ativos Conta da AWS adquiridos associados ao usuário

`ElementalActivationsReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ElementalActivationsReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 28 de agosto de 2020, 16:51 UTC
- Hora da edição: 28 de agosto de 2020, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ElementalAppliancesSoftwareFullAccess

Descrição: acesso total para visualizar e agir sobre cotações e pedidos de dispositivos e software do Elemental

`ElementalAppliancesSoftwareFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ElementalAppliancesSoftwareFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 31 de julho de 2019, 16:28 UTC
- Hora da edição: 05 de fevereiro de 2021, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ElementalAppliancesSoftwareReadOnlyAccess

Descrição: Read-only acesso para visualizar cotações e pedidos de Elemental Appliances and Software

`ElementalAppliancesSoftwareReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ElementalAppliancesSoftwareReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 01 de abril de 2020, 22:31 UTC
- Hora da edição: 01 de abril de 2020, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:List*",
        "elemental-appliances-software:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ElementalSupportCenterFullAccess

Descrição: acesso total para visualizar e agir sobre casos de suporte de dispositivos e software do Elemental e conteúdo de suporte a produtos

`ElementalSupportCenterFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ElementalSupportCenterFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de novembro de 2020, 18:08 UTC
- Hora da edição: 05 de fevereiro de 2021, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

EMRDescribeClusterPolicyForEMRWAL

Descrição: esta política concede permissões somente leitura que permitem que o serviço WAL para Amazon EMR encontre e retorne o status de um cluster

`EMRDescribeClusterPolicyForEMRWAL` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 15 de junho de 2023, 23:30 UTC
- Hora da edição: 15 de junho de 2023, 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

EndUserMessagingServiceRolePolicy

Descrição: Permite EndUserMessaging publicar métricas CloudWatch em seu nome

`EndUserMessagingServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 29 de setembro de 2026, 19:37 UTC
- Horário editado: 29 de setembro de 2026, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EndUserMessagingServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/EndUserMessaging"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

FinOpsAgentAgentPolicy

Descrição: Fornece as permissões exigidas pelo AWS FinOps agente para realizar análises de custos e identificar oportunidades de economia de custos nos AWS recursos do cliente.

`FinOpsAgentAgentPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `FinOpsAgentAgentPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de junho de 2026, 19:57 UTC
- Horário editado: 02 de outubro de 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/FinOpsAgentAgentPolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FinOpsAgentDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageWithResources",
        "ce:GetCostForecast",
        "ce:GetUsageForecast",
        "ce:GetDimensionValues",
```

```
        "ce:GetTags",
        "ce:GetCostCategories",
        "ce:GetCostAndUsageComparisons",
        "ce:GetCostComparisonDrivers",
        "ce:GetSavingsPlansCoverage",
        "ce:GetSavingsPlansUtilization",
        "ce:GetSavingsPlansUtilizationDetails",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "ce:GetReservationCoverage",
        "ce:GetReservationUtilization",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetAnomalies",
        "ce:GetAnomalyMonitors",
        "ce:ListCostAllocationTags",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:DescribeCostCategoryDefinition",
        "ce:ListCostCategoryDefinitions",
        "ce:StartCommitmentPurchaseAnalysis",
        "ce:ListCommitmentPurchaseAnalyses",
        "ce:GetCommitmentPurchaseAnalysis",
        "ce:StartSavingsPlansPurchaseRecommendationGeneration",
        "ce:ListSavingsPlansPurchaseRecommendationGeneration",
        "ce:GetSavingsPlanPurchaseRecommendationDetails",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetRecommendationSummaries",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendations",
```

```
        "compute-optimizer:GetRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:GetIdleRecommendations",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:ListServices",
        "ecs:ListClusters",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "lambda:ListFunctions",
        "lambda:ListProvisionedConcurrencyConfigs",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBMajorEngineVersions",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts",
        "freetier:GetFreeTierUsage",
        "bcm-pricing-calculator:GetPreferences",
        "bcm-pricing-calculator:GetWorkloadEstimate",
        "bcm-pricing-calculator:ListWorkloadEstimateUsage",
        "bcm-pricing-calculator:ListWorkloadEstimates",
        "cloudtrail:LookupEvents",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "logs:StartQuery",
        "logs:GetQueryResults",
        "billing:GetBillingView",
        "billing:GetEnterpriseSupportChargeSummary",
        "billing:GetEnterpriseSupportContractDetails",
        "billing:ListBillingViews",
        "billing:ListEnterpriseSupportLinkedAccountCharges",
        "billing:ListSourceViewsForBillingView",
        "billing:GetResourcePolicy",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroupCostReports",
        "billingconductor:GetBillingGroupCostReport",
```

```
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListCustomLineItemVersions",
        "billingconductor:ListResourcesAssociatedToCustomLineItem",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListPricingPlansAssociatedWithPricingRule",
        "invoicing:ListInvoiceSummaries",
        "invoicing:ListInvoiceUnits",
        "invoicing:GetInvoiceUnit",
        "invoicing:BatchGetInvoiceProfile",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:GetProcurementPortalPreference",
        "aco-automation:GetAutomationEvent",
        "aco-automation:GetAutomationRule",
        "aco-automation:GetEnrollmentConfiguration",
        "aco-automation:ListAccounts",
        "aco-automation:ListAutomationEvents",
        "aco-automation:ListAutomationEventSteps",
        "aco-automation:ListAutomationEventSummaries",
        "aco-automation:ListAutomationRules",
        "aco-automation:ListRecommendedActions",
        "aco-automation:ListRecommendedActionSummaries",
        "aco-automation:ListAutomationRulePreview",
        "aco-automation:ListAutomationRulePreviewSummaries",
        "aco-automation:ListTagsForResource",
        "billing:GetCredits",
        "billing:GetCreditAllocationHistory",
        "health:DescribeEvents",
        "savingsplans:DescribeSavingsPlans",
        "savingsplans:DescribeSavingsPlanRates",
        "savingsplans:DescribeSavingsPlansOfferings",
        "savingsplans:DescribeSavingsPlansOfferingRates",
        "savingsplans:ListTagsForResource",
        "cost-optimization-hub:ListEfficiencyMetrics",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:GetPreferences",
        "billing:GetBillingPreferences",
        "billing:ListBillingViewSegments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridgeManagedRuleManagementWritePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:EnableRule",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "finops-agent.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EventBridgeManagedRuleManagementReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

FinOpsAgentOperatorPolicy

Descrição: Fornece acesso para usar o aplicativo web AWS FinOps Agent para um agente.

`FinOpsAgentOperatorPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `FinOpsAgentOperatorPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de junho de 2026, 19:57 UTC
- Horário editado: 03 de junho de 2026, 19:57 UTC
- ARN: `arn:aws:iam::aws:policy/FinOpsAgentOperatorPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FinOpsAgentOperatorAccess",
      "Effect" : "Allow",
      "Action" : [
        "finops-agent:CreateConversation",
        "finops-agent:ListConversations",
        "finops-agent:CreateTurn",
        "finops-agent:GetTurn",
```

```
        "finops-agent:ListTurns",
        "finops-agent:CancelTurn",
        "finops-agent:AcceptAgentRequest",
        "finops-agent:RejectAgentRequest",
        "finops-agent:GetAgentRequest",
        "finops-agent:CreateTask",
        "finops-agent:GetTask",
        "finops-agent:ListTasks",
        "finops-agent:CancelTask",
        "finops-agent:CreateAutomation",
        "finops-agent:GetAutomation",
        "finops-agent:ListAutomations",
        "finops-agent:UpdateAutomation",
        "finops-agent:DeleteAutomation",
        "finops-agent:CreateDocument",
        "finops-agent:GetDocumentContent",
        "finops-agent:GetDocumentMetadata",
        "finops-agent:ListDocuments",
        "finops-agent:UpdateDocument",
        "finops-agent:DeleteDocument",
        "finops-agent:RestoreDocument",
        "finops-agent:GetArtifactContent",
        "finops-agent:GetArtifactMetadata",
        "finops-agent:DeleteArtifact",
        "finops-agent:ListArtifacts",
        "finops-agent:ListRecords",
        "finops-agent:SendFeedback"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

FMSServiceRolePolicy

Descrição: Política de acesso para permitir que a função vinculada ao serviço FM realize FM-related ações em FM-managed recursos dentro de uma conta AWS da organização do cliente.

`FMSServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 28 de março de 2018, 23:01 UTC
- Horário editado: 06 de abril de 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy`

Versão da política

Versão da política: v37 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WafGeneral",
      "Effect" : "Allow",
      "Action" : [
        "waf:UpdateWebACL",
        "waf:DeleteWebACL",
        "waf:GetWebACL",
```

```
        "waf:GetRuleGroup",
        "waf:ListSubscribedRuleGroups",
        "waf-regional:UpdateWebACL",
        "waf-regional:DeleteWebACL",
        "waf-regional:GetWebACL",
        "waf-regional:GetRuleGroup",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:AssociateWebACL",
        "waf-regional:DisassociateWebACL",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "elasticloadbalancing:SetSecurityGroups",
        "waf:ListTagsForResource",
        "waf-regional:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*"
      ]
    },
    {
      "Sid" : "Wafv2Logging",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/webacl/*"
      ]
    },
    {
      "Sid" : "WafWebaclCreation",
      "Effect" : "Allow",
      "Action" : [
        "waf:CreateWebACL",
```

```
        "waf-regional:CreateWebACL",
        "waf:GetChangeToken",
        "waf-regional:GetChangeToken",
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:*",
        "arn:aws:waf-regional:*:*:*"
      ]
    },
    {
      "Sid" : "ElbGeneral",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "WafPermissionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "waf:PutPermissionPolicy",
        "waf:GetPermissionPolicy",
        "waf:DeletePermissionPolicy",
        "waf-regional:PutPermissionPolicy",
        "waf-regional:GetPermissionPolicy",
        "waf-regional:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:rulegroup/*"
      ]
    },
    {
      "Sid" : "CloudfrontGeneral",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "cloudfront:UpdateDistribution",
        "cloudfront:ListDistributionsByWebACLId",
```

```
        "cloudfront:ListDistributions",
        "cloudfront:ListTagsForResource",
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:DisassociateDistributionWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudfrontVpcOriginAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetVpcOrigin"
      ],
      "Resource" : "arn:aws:cloudfront::*:vpcorigin/*"
    },
    {
      "Sid" : "ConfigScoped",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:StartConfigRulesEvaluation",
        "config:DeleteEvaluationResults"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/fms.amazonaws.com/
*"
    },
    {
      "Sid" : "ConfigUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:PutConfigurationRecorder",
        "config:StartConfigurationRecorder",
        "config:PutDeliveryChannel",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetComplianceSummaryByConfigRule",
        "config:GetDiscoveredResourceCounts",
```

```
        "config:PutEvaluations",
        "config:SelectResourceConfig",
        "config:BatchGetResourceConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/fms.amazonaws.com/AWSServiceRoleForFMS"
      ]
    },
    {
      "Sid" : "OrganizationsGeneral",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ShieldGeneral",
      "Effect" : "Allow",
      "Action" : [
        "shield:CreateProtection",
        "shield:DeleteProtection",
        "shield:DescribeProtection",
        "shield:ListProtections",
        "shield:ListAttacks",
```

```
        "shield:CreateSubscription",
        "shield:DescribeSubscription",
        "shield:GetSubscriptionState",
        "shield:DescribeDRTAccess",
        "shield:DescribeEmergencyContactSettings",
        "shield:UpdateEmergencyContactSettings",
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeAddresses",
        "shield:EnableApplicationLayerAutomaticResponse",
        "shield:DisableApplicationLayerAutomaticResponse",
        "shield:UpdateApplicationLayerAutomaticResponse"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2SecurityGroupScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "SecurityGroupTagCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
```

```
        }
      }
    },
    {
      "Sid" : "SecurityGroupTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/FMManaged" : "*"
        }
      }
    },
    {
      "Sid" : "Ec2Unscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeInstances",
        "ec2:AssociateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DisassociateRouteTable",
        "ec2:ReplaceRouteTableAssociation"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "Wafv2General",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:TagResource",
        "wafv2:ListResourcesForWebACL",
        "wafv2:AssociateWebACL",
        "wafv2:ListTagsForResource",
        "wafv2:UntagResource",
        "wafv2:GetWebACL",
        "wafv2:DisassociateFirewallManager",
        "wafv2:DeleteWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Sid" : "Wafv2WebAclAndRuleGroupMutation",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:UpdateWebACL",
        "wafv2:CreateWebACL",
        "wafv2:DeleteFirewallManagerRuleGroups",
        "wafv2:PutFirewallManagerRuleGroups"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/ipset/*",
        "arn:aws:wafv2:*:*:regional/ipset/*",
        "arn:aws:wafv2:*:*:global/regexpatternset/*",
        "arn:aws:wafv2:*:*:regional/regexpatternset/*"
      ]
    },
    {
      "Sid" : "Wafv2PermissionPolicy",
      "Effect" : "Allow",
```

```
      "Action" : [
        "wafv2:PutPermissionPolicy",
        "wafv2:GetPermissionPolicy",
        "wafv2:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*"
      ]
    },
    {
      "Sid" : "Wafv2WebaclDescribe",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Sid" : "RouteTableTagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateRouteTable"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "SubnetTagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
```

```
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "VPCEndpointTagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RouteTableCleanup",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteRouteTable",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInternetGateways",
```

```
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateVpcEndpointScoped",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Sid" : "CreateVpcEndpointUnscoped",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "VpcEndpointsDeletion",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "RamTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:resource-share/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RamMutation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RamCreation",
      "Effect" : "Allow",
      "Action" : "ram:CreateResourceShare",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
```

```
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Sid" : "RamDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "network-firewall.amazonaws.com",
            "shield.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamDescribe",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:TagResource"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "NetworkFirewallGeneral",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:AssociateSubnets",
        "network-firewall:CreateFirewall",
        "network-firewall:CreateFirewallPolicy",
        "network-firewall:DisassociateSubnets",
        "network-firewall:UpdateFirewallDeleteProtection",
        "network-firewall:UpdateFirewallPolicy",
        "network-firewall:UpdateFirewallPolicyChangeProtection",
        "network-firewall:UpdateSubnetChangeProtection",
        "network-firewall:AssociateFirewallPolicy",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DeleteResourcePolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:UpdateLoggingConfiguration",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:ListTLSInspectionConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:PutResourcePolicy"
      ],
```

```
      "Resource" : [
        "arn:aws:network-firewall:*:*:firewall-policy/*",
        "arn:aws:network-firewall:*:*:stateful-rulegroup/*",
        "arn:aws:network-firewall:*:*:stateless-rulegroup/*"
      ]
    },
    {
      "Sid" : "NetworkFirewallCleanup",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DeleteFirewallPolicy",
        "network-firewall:DeleteFirewall"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LogsGeneral",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53ResolverRuleGroupUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListTagsForResource",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupPolicy",
        "route53resolver:PutFirewallRuleGroupPolicy"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "Route53ResolverRuleGroupCleanup",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:UpdateFirewallRuleGroupAssociation",
        "route53resolver:DisassociateFirewallRuleGroup"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Route53ResolverRuleGroupScoped",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:AssociateFirewallRuleGroup",
        "route53resolver:TagResource"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclTagCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged",
            "FMPolicies"
          ]
```

```
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkAcl"
        }
      }
    },
    {
      "Sid" : "NaclTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged",
            "FMPolicies"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkAclEntry",
        "ec2:CreateNetworkAclEntry",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "NaclUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:DescribeNetworkAcls",
        "ec2:CreateNetworkAcl"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

FSxDeleteServiceLinkedRoleAccess

Descrição: permite que o Amazon FSx exclua seus perfis vinculados ao serviço para acesso ao Amazon S3

`FSxDeleteServiceLinkedRoleAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 28 de novembro de 2018, 10:40 UTC
- Hora da edição: 28 de novembro de 2018, 10:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetRole"
      ],
      "Resource" : "arn:*:iam::*:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

GameLiftContainerFleetPolicy

Descrição: Concede as permissões necessárias para ações computacionais em uma frota de GameLift contêineres da Amazon, incluindo acesso a dependências como o Amazon S3.

`GameLiftContainerFleetPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `GameLiftContainerFleetPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 12 de novembro de 2024, 19:28 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftContainerFleetPolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WriteGameSessionLogsToLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:gamelift-*:log-stream:*"
    },
    {
      "Sid" : "CreateLogGroupToStoreGameSessionLogs",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:gamelift-*"
    },
```

```
    {
      "Sid" : "WriteGameSessionLogsToS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::gamelift-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RetrieveComputeAuthToken",
      "Effect" : "Allow",
      "Action" : [
        "gamelift:GetComputeAuthToken"
      ],
      "Resource" : [
        "arn:aws:gamelift:*:*:containerfleet/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

GameLiftGameServerGroupPolicy

Descrição: Política para permitir que a Gamelift gerencie GameServerGroups os recursos do cliente

`GameLiftGameServerGroupPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `GameLiftGameServerGroupPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 03 de abril de 2020, 23:12 UTC
- Hora da edição: 13 de maio de 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/GameLift" : "GameServerGroups"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:EnterStandby",
```

```
        "autoscaling:SetInstanceProtection",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SuspendProcesses",
        "autoscaling:DetachInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/GameLift" : "GameServerGroups"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sns:Publish",
      "Resource" : [
        "arn:*:sns:*:*:ActivatingLifecycleHookTopic-*",
        "arn:*:sns:*:*:TerminatingLifecycleHookTopic-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/GameLift"
        }
      }
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

GitLabDuoWithAmazonQPermissionsPolicy

Descrição: Essa política gerenciada concede permissão para se conectar ao Amazon Q e utilizar os recursos da integração do GitLab Duo com o Amazon Q.

`GitLabDuoWithAmazonQPermissionsPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `GitLabDuoWithAmazonQPermissionsPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 16 de abril de 2025, 16:37 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/GitLabDuoWithAmazonQPermissionsPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GitLabDuoUsagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:SendEvent",
        "q:CreateAuthGrant",
        "q:UpdateAuthGrant",
        "q:GenerateCodeRecommendations",
        "q:SendMessage",
        "q:ListPlugins",
        "q:VerifyOAuthAppConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GitLabDuoManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:CreateOAuthAppConnection",
        "q:DeleteOAuthAppConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GitLabDuoPluginPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:CreatePlugin",
        "q:DeletePlugin",
        "q:GetPlugin"
      ],
      "Resource" : "arn:aws:qdeveloper:*:*:plugin/GitLabDuoWithAmazonQ/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

GlobalAcceleratorFullAccess

Descrição: Permitir que GlobalAccelerator os usuários tenham acesso total a todas as APIs

`GlobalAcceleratorFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `GlobalAcceleratorFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de novembro de 2018, 2:44 UTC
- Hora da edição: 04 de dezembro de 2020, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Action" : [
        "globalaccelerator:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRegions",
        "ec2:DescribeSubnets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "globalaccelerator.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

GlobalAcceleratorReadOnlyAccess

Descrição: Permitir que GlobalAccelerator os usuários acessem APIs somente para leitura

`GlobalAcceleratorReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `GlobalAcceleratorReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de novembro de 2018, 2:41 UTC
- Hora da edição: 27 de novembro de 2018, 2:41 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:Describe*",
        "globalaccelerator:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

GreengrassOTAUpdateArtifactAccess

Descrição: fornece acesso de leitura aos artefatos do Greengrass OTA Update em todas as regiões do Greengrass

`GreengrassOTAUpdateArtifactAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `GreengrassOTAUpdateArtifactAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 29 de novembro de 2017, 18:11 UTC
- Hora da edição: 18 de dezembro de 2018, 0:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

GroundTruthSyntheticConsoleFullAccess

Descrição: Essa política concede as permissões necessárias para usar todos os recursos do SageMaker Ground Truth Synthetic Console.

`GroundTruthSyntheticConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `GroundTruthSyntheticConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de agosto de 2022, 15:58 UTC
- Hora da edição: 25 de agosto de 2022, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

GroundTruthSyntheticConsoleReadOnlyAccess

Descrição: Esta política concede acesso somente para leitura ao SageMaker Ground Truth Synthetic por meio do. Console de gerenciamento da AWS

`GroundTruthSyntheticConsoleReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `GroundTruthSyntheticConsoleReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 25 de agosto de 2022, 15:58 UTC
- Hora da edição: 25 de agosto de 2022, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

Health_OrganizationsServiceRolePolicy

Descrição: Política AWS de saúde para ativar o recurso de visualização organizacional

`Health_OrganizationsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 16 de dezembro de 2019, 13:28 UTC
- Hora da edição: 6 de fevereiro de 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

IAMAccessAdvisorReadOnly

Descrição: esta política concede acesso para ler todas as informações de acesso fornecidas pelo consultor de acesso do IAM, como as informações do último acesso do serviço.

`IAMAccessAdvisorReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `IAMAccessAdvisorReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 21 de junho de 2019, 19:33 UTC
- Hora da edição: 21 de junho de 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListPolicies",
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GenerateOrganizationsAccessReport",
        "iam:GenerateCredentialReport",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetailsWithEntities",
        "iam:GetOrganizationsAccessReport",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
```

```
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListPolicies",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

IAMAccessAnalyzerFullAccess

Descrição: fornece acesso total a recursos do IAM Access Analyzer.

`IAMAccessAnalyzerFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `IAMAccessAnalyzerFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 02 de dezembro de 2019, 17:12 UTC
- Hora da edição: 02 de dezembro de 2019, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "access-analyzer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
```

```
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

IAMAccessAnalyzerReadOnlyAccess

Descrição: fornece acesso somente leitura a recursos do IAM Access Analyzer.

`IAMAccessAnalyzerReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `IAMAccessAnalyzerReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 02 de dezembro de 2019, 17:12 UTC
- Hora da edição: 18 de julho de 2024, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMAccessAnalyzerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:Get*",
        "access-analyzer:List*",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

IAMFullAccess

Descrição: Fornece acesso total ao IAM por meio do Console de gerenciamento da AWS.

`IAMFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `IAMFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 21 de junho de 2019, 19:40 UTC
- ARN: `arn:aws:iam::aws:policy/IAMFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:*",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListPolicies",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

IAMReadOnlyAccess

Descrição: fornece acesso somente para leitura ao IAM por meio do Console de gerenciamento da AWS.

`IAMReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `IAMReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:40 UTC
- Hora da edição: 25 de janeiro de 2018, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/IAMReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

IAMSelfManageServiceSpecificCredentials

Descrição: permite que um usuário do IAM gerencie suas próprias credenciais específicas de serviço.

`IAMSelfManageServiceSpecificCredentials` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `IAMSelfManageServiceSpecificCredentials` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 22 de dezembro de 2016, 17:25 UTC

- Hora da edição: 22 de dezembro de 2016, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:ListServiceSpecificCredentials",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

IAMUserChangePassword

Descrição: permite que um usuário do IAM altere sua própria senha.

`IAMUserChangePassword` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `IAMUserChangePassword` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 15 de novembro de 2016, 0:25 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserChangePassword`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}",
        "arn:aws:iam::*:user/*/${aws:username}"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

IAMUserSSHKeys

Descrição: permite que um usuário do IAM gerencie suas próprias chaves SSH.

`IAMUserSSHKeys` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `IAMUserSSHKeys` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de julho de 2015, 17:08 UTC
- Hora da edição: 09 de julho de 2015, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserSSHKeys`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

IVSFullAccess

Descrição: fornece acesso total ao Interactive Video Service (IVS). Também inclui permissões para serviços dependentes, necessários para acesso total ao console do IVS.

`IVSFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `IVSFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 13 de dezembro de 2023, 21:20 UTC
- Hora da edição: 13 de dezembro de 2023, 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:*",
        "ivschat:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

IVSReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao IVS e às APIs de streaming Low-Latency Real-Time

`IVSReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `IVSReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 5 dezembro de 2023, 18:00 UTC
- Horário editado: 25 de setembro de 2026, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSReadOnlyAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ivs:BatchGetChannel",
        "ivs:GetAdConfiguration",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetIngestConfiguration",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetPublicKey",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetStorageConfiguration",
        "ivs:GetStream",
        "ivs:GetStreamSession",
        "ivs:ListAdConfigurations",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListParticipants",
        "ivs:ListParticipantReplicas",
        "ivs:ListParticipantEvents",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStageSessions",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

IVSRecordToS3

Descrição: Função vinculada ao serviço para executar S3 PutObject para gravar transmissões ao vivo do IVS

`IVSRecordToS3` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 05 de dezembro de 2020, 0:10 UTC
- Hora da edição: 05 de dezembro de 2020, 0:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

KafkaConnectServiceRolePolicy

Descrição: Essa política concede ao Kafka Connect permissão para gerenciar AWS recursos em seu nome.

`KafkaConnectServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 07 de setembro de 2021, 13:12 UTC

- Hora da edição: 07 de setembro de 2021, 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonMSKConnectManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "AmazonMSKConnectManaged"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonMSKConnectManaged" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

KafkaServiceRolePolicy

Descrição: política de perfil vinculado ao serviço do IAM para Kafka

`KafkaServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 15 de novembro de 2018, 23:31 UTC
- Horário editado: 10 de novembro de 2025, 23:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AttachNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeVpcEndpoints",
        "acm-pca:GetCertificateAuthorityCertificate",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:*:ec2:*:*:subnet/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "secretsmanager:SecretId" : "arn:*:secretsmanager:*:*:secret:AmazonMSK_*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses",
```

```
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:*:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

KeyspacesCDCServiceRolePolicy

Descrição: concede as permissões necessárias ao Amazon Keyspaces para captura de dados de alterações.

`KeyspacesCDCServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 21 de junho de 2025, 00:22 UTC
- Horário editado: 21 de junho de 2025, 00:22 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesCDCServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KeyspacesPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Cassandra"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

KeyspacesReplicationServiceRolePolicy

Descrição: permissões exigidas pelo Keyspaces para replicação de dados entre regiões

`KeyspacesReplicationServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 02 de maio de 2023, 16:15 UTC
- Horário editado: 15 de novembro de 2024, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KeyspacesActionsNeededForSteadyStateReplication",
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:Modify",
        "cassandra:Alter",
```

```
        "cassandra:ModifyMultiRegionResource",
        "cassandra:SelectMultiRegionResource",
        "cassandra:AlterMultiRegionResource",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWDeleteAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking-*"
    },
    {
      "Sid" : "CWDescribeAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "CWPutMetricAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking-*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "cloudwatch:AlarmActions" : [
            "arn:aws:autoscaling:*:*:scalingPolicy:*:resource/cassandra/keyspace/*/
table/*:policyName/*:createdBy/*"
          ]
        }
      }
    }
  ]
```

```
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

LakeFormationDataAccessServiceRolePolicy

Descrição: política para conceder acesso temporário aos dados de recursos do Lake Formation

`LakeFormationDataAccessServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 20 de junho de 2019, 20:46 UTC
- Hora da edição: 6 de fevereiro de 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

LexBotPolicy

Descrição: Política para o caso de uso do AWS Lex Bot

`LexBotPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 17 de fevereiro de 2017, 22:18 UTC
- Hora da edição: 13 de novembro de 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectSentiment"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

LexChannelPolicy

Descrição: Política para o caso de uso do AWS Lex Channel

`LexChannelPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 17 de fevereiro de 2017, 23:23 UTC
- Hora da edição: 17 de fevereiro de 2017, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:PostText"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

LightsailExportAccess

Descrição: Política de função vinculada ao serviço AWS Lightsail que concede permissões para exportar recursos

`LightsailExportAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 28 de setembro de 2018, 16:35 UTC
- Hora da edição: 15 de janeiro de 2022, 1:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot",
        "ec2:DescribeSnapshots",
        "ec2:CopyImage",
        "ec2:DescribeImages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

MediaConnectGatewayInstanceRolePolicy

Descrição: Essa política concede permissão para registrar instâncias de MediaConnect gateway em um MediaConnect gateway.

`MediaConnectGatewayInstanceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `MediaConnectGatewayInstanceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 22 de março de 2023, 20:43 UTC
- Hora da edição: 22 de março de 2023, 20:43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:PollGateway",
        "mediaconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

MediaPackageServiceRolePolicy

Descrição: MediaPackage Permite publicar registros em CloudWatch

`MediaPackageServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 18 de setembro de 2020, 17:45 UTC
- Hora da edição: 18 de setembro de 2020, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

MemoryDBServiceRolePolicy

Descrição: Essa política permite que o MemoryDB gerencie AWS recursos em seu nome conforme necessário para gerenciar seus recursos.

`MemoryDBServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 17 de agosto de 2021, 22:34 UTC
- Horário editado: 01 de dezembro de 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateMemoryDBTagsOnNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonMemoryDBManaged"
          ]
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaces",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "DeleteMemoryDBTaggedNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonMemoryDBManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "DescribeEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "PutCloudWatchMetricData",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/MemoryDB"
        }
      }
    },
    {
      "Sid" : "ReplicateMemoryDBMultiRegionClusterData",
      "Effect" : "Allow",
      "Action" : [
        "memorydb:ReplicateMultiRegionClusterData"
      ],
      "Resource" : "arn:aws:memorydb:*:*:cluster/*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

MigrationHubDMSAccessServiceRolePolicy

Descrição: política que permite que o Database Migration Service assuma um perfil na conta do cliente para chamar o Migration Hub

`MigrationHubDMSAccessServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 12 de junho de 2019, 17:50 UTC
- Hora da edição: 07 de outubro de 2019, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
        "mgh:ListDiscoveredResources",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
```

```
        "mgh:DisassociateDiscoveredResource",
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

MigrationHubServiceRolePolicy

Descrição: permite que o Migration Hub chame o Application Discovery Service em seu nome

`MigrationHubServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função

- Hora da criação: 12 de junho de 2019, 17:22 UTC
- Hora da edição: 06 de agosto de 2020, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "dms:AddTagsToResource",
      "Resource" : [
        "arn:aws:dms:*:*:endpoint:*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

MigrationHubSMSAccessServiceRolePolicy

Descrição: política que permite que o Server Migration Service assuma um perfil na conta do cliente para chamar o Migration Hub

`MigrationHubSMSAccessServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 12 de junho de 2019, 18:30 UTC
- Hora da edição: 07 de outubro de 2019, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
        "mgh:ListDiscoveredResources",
```

```
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:DisassociateDiscoveredResource",
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

MonitronServiceRolePolicy

Descrição: Política para a função vinculada ao serviço AWS Monitron que concede acesso aos recursos necessários do cliente.

`MonitronServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 02 de maio de 2022, 19:22 UTC
- Hora da edição: 02 de maio de 2022, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

MultiPartyApprovalFullAccess

Descrição: Fornece acesso total à Multi-party aprovação. Essa política também inclui permissões relacionadas às AWS organizações e à identidade AWS do IAM para gerenciar equipes de aprovação e fontes de identidade.

`MultiPartyApprovalFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `MultiPartyApprovalFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 18 de junho de 2025, 20:22 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/MultiPartyApprovalFullAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MpaFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "mpa:*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOCreateApplication",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication"
      ],
      "Resource" : [
        "arn:aws:sso:::instance/*",
        "arn:aws:sso::aws:applicationProvider/mpa"
      ]
    },
    {
      "Sid" : "SSOApplicationManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationAccessScope",
        "sso:DeleteApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "mpa.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeInstance",
        "sso:DescribeRegisteredRegions",
```

```
        "sso:GetSharedSsoConfiguration",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "sso:ListInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

MultiPartyApprovalReadOnlyAccess

Descrição: Fornece acesso somente para Multi-party leitura à aprovação. Essa política também inclui permissão de leitura relacionada às AWS organizações e à identidade AWS do IAM para equipes de aprovação e fontes de identidade.

`MultiPartyApprovalReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `MultiPartyApprovalReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 18 de junho de 2025, 20:07 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/MultiPartyApprovalReadOnlyAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MpaReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "mpa:Get*",
        "mpa:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

NeptuneConsoleFullAccess

Descrição: fornece acesso total para gerenciar o Amazon Neptune usando o Console de gerenciamento da AWS. Observe que essa política também concede acesso total para publicar em todos os tópicos do SNS dentro da conta, permissões para criar e editar instâncias do Amazon EC2 e configurações de VPC, permissões para visualizar e listar chaves no Amazon KMS e acesso total ao Amazon RDS. Para obter mais informações, consulte https://aws.amazon.com/neptune/faqs/..

`NeptuneConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `NeptuneConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 19 de junho de 2018, 21:35 UTC
- Hora da edição: 30 de novembro de 2023, 7:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
```

```
            "neptune"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
```

```
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOtherDepedentPermissions",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
```

```
        "ec2:AttachNetworkInterface",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "iam:ListRoles",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
```

```
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForNeptune",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateSLRForNeptune",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForNeptuneAnalytics",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:CreateGraph",
        "neptune-graph:DeleteGraph",
        "neptune-graph:GetGraph",
        "neptune-graph:ListGraphs",
        "neptune-graph:UpdateGraph",
        "neptune-graph:ResetGraph",
```

```
        "neptune-graph:CreateGraphSnapshot",
        "neptune-graph:DeleteGraphSnapshot",
        "neptune-graph:GetGraphSnapshot",
        "neptune-graph:ListGraphSnapshots",
        "neptune-graph:RestoreGraphFromSnapshot",
        "neptune-graph:CreatePrivateGraphEndpoint",
        "neptune-graph:GetPrivateGraphEndpoint",
        "neptune-graph:ListPrivateGraphEndpoints",
        "neptune-graph:DeletePrivateGraphEndpoint",
        "neptune-graph:CreateGraphUsingImportTask",
        "neptune-graph:GetImportTask",
        "neptune-graph:ListImportTasks",
        "neptune-graph:CancelImportTask"
      ],
      "Resource" : [
        "arn:aws:neptune-graph:*:*:*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForNeptuneAnalytics",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "neptune-graph.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateSLRForNeptuneAnalytics",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "neptune-graph.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

NeptuneFullAccess

Descrição: fornece acesso total ao Amazon Neptune. Observe que essa política também concede acesso total para publicar em todos os tópicos do SNS dentro da conta e acesso total ao Amazon RDS. Para obter mais informações, consulte https://aws.amazon.com/neptune/faqs/..

`NeptuneFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `NeptuneFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de maio de 2018, 19:17 UTC
- Hora da edição: 22 de janeiro de 2024, 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
            "neptune"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBClusterEndpoint",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterEndpoint",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
```

```
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DeleteGlobalCluster",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:FailoverGlobalCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterEndpoint",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:ModifyGlobalCluster",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
```

```
        "rds:RemoveFromGlobalCluster",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:StartDBCluster",
        "rds:StopDBCluster"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOtherDepedentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForNeptune",
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateSLRForNeptune",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowDataAccessForNeptune",
      "Effect" : "Allow",
      "Action" : [
        "neptune-db:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

NeptuneGraphReadOnlyAccess

Descrição: fornece acesso somente leitura a todos os recursos do Amazon Neptune Analytics, além de permissões somente leitura para serviços dependentes.

`NeptuneGraphReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `NeptuneGraphReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de novembro de 2023, 7:32 UTC
- Hora da edição: 30 de novembro de 2023, 7:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForNeptuneGraph",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:Get*",
        "neptune-graph:List*",
        "neptune-graph:Read*"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    }
```

```
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

NeptuneReadOnlyAccess

Descrição: fornece acesso somente leitura ao Amazon Neptune. Observe que essa política também concede acesso a recursos do Amazon RDS. Para obter mais informações, consulte https://aws.amazon.com/neptune/faqs/..

`NeptuneReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `NeptuneReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de maio de 2018, 19:16 UTC
- Hora da edição: 22 de janeiro de 2024, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowReadOnlyPermissionsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "kms:ListAliases",
        "kms:ListKeyPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForNeptuneDB",
      "Effect" : "Allow",
      "Action" : [
        "neptune-db:Read*",
        "neptune-db:Get*",
        "neptune-db:List*"
      ],
```

```
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

NetworkAdministrator

Descrição: Concede permissões de acesso total aos AWS serviços e ações necessários para instalar e configurar recursos AWS de rede.

`NetworkAdministrator` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `NetworkAdministrator` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de trabalho
- Hora da criação: 10 de novembro de 2016, 17:31 UTC
- Horário editado: 09 de julho de 2026, 14:42 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/NetworkAdministrator`

Versão da política

Versão da política: v16 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDefaultNetworkAdminActions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudfront:ListDistributions",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "directconnect:*",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:CreateCarrierGateway",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateFlowLogs",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
```

```
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpointConnectionNotification",
        "ec2:CreateVpcEndpointServiceConfiguration",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteCarrierGateway",
        "ec2:DeleteEgressOnlyInternetGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpointConnectionNotifications",
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeKeyPairs",
```

```
            "ec2:DescribeMovingAddresses",
            "ec2:DescribeNatGateways",
            "ec2:DescribeNetworkAcls",
            "ec2:DescribeNetworkInterfaceAttribute",
            "ec2:DescribeNetworkInterfacePermissions",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribePlacementGroups",
            "ec2:DescribePrefixLists",
            "ec2:DescribePublicIpv4Pools",
            "ec2:DescribeRouteTables",
            "ec2:DescribeSecurityGroupReferences",
            "ec2:DescribeSecurityGroupRules",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeStaleSecurityGroups",
            "ec2:DescribeSubnets",
            "ec2:DescribeTags",
            "ec2:DescribeVpcAttribute",
            "ec2:DescribeVpcClassicLink",
            "ec2:DescribeVpcClassicLinkDnsSupport",
            "ec2:DescribeVpcEndpointConnectionNotifications",
            "ec2:DescribeVpcEndpointConnections",
            "ec2:DescribeVpcEndpointServiceConfigurations",
            "ec2:DescribeVpcEndpointServicePermissions",
            "ec2:DescribeVpcEndpointServices",
            "ec2:DescribeVpcEndpoints",
            "ec2:DescribeVpcPeeringConnections",
            "ec2:DescribeVpcs",
            "ec2:DescribeVpnConnections",
            "ec2:DescribeVpnGateways",
            "ec2:DetachInternetGateway",
            "ec2:DetachNetworkInterface",
            "ec2:DetachVpnGateway",
            "ec2:DisableVgwRoutePropagation",
            "ec2:DisableVpcClassicLinkDnsSupport",
            "ec2:DisassociateAddress",
            "ec2:DisassociateRouteTable",
            "ec2:DisassociateSubnetCidrBlock",
            "ec2:DisassociateVpcCidrBlock",
            "ec2:EnableVgwRoutePropagation",
            "ec2:EnableVpcClassicLinkDnsSupport",
            "ec2:GetVpnConnectionDeviceSampleConfiguration",
            "ec2:GetVpnConnectionDeviceTypes",
            "ec2:GetVpnTunnelReplacementStatus",
            "ec2:ModifyNetworkInterfaceAttribute",
```

```
        "ec2:ModifySecurityGroupRules",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ModifyVpcEndpointConnectionNotification",
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:ModifyVpcPeeringConnectionOptions",
        "ec2:ModifyVpcTenancy",
        "ec2:ModifyVpnConnection",
        "ec2:ModifyVpnConnectionOptions",
        "ec2:ModifyVpnTunnelCertificate",
        "ec2:ModifyVpnTunnelOptions",
        "ec2:MoveAddressToVpc",
        "ec2:RejectVpcEndpointConnections",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:ReplaceVpnTunnel",
        "ec2:ResetNetworkInterfaceAttribute",
        "ec2:RestoreAddressToClassic",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticloadbalancing:*",
        "interconnect:AcceptConnectionProposal",
        "interconnect:CreateConnection",
        "interconnect:DeleteConnection",
        "interconnect:DescribeConnectionProposal",
        "interconnect:GetConnection",
        "interconnect:GetEnvironment",
        "interconnect:ListAttachPoints",
        "interconnect:ListConnections",
        "interconnect:ListEnvironments",
        "interconnect:ListTagsForResource",
        "interconnect:TagResource",
        "interconnect:UntagResource",
```

```
        "interconnect:UpdateConnection",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "route53:*",
        "route53domains:*",
        "sns:CreateTopic",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowVPCPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AssociateSecurityGroupVpc",
        "ec2:AttachClassicLinkVpc",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DetachClassicLinkVpc",
        "ec2:DisableVpcClassicLink",
        "ec2:DisassociateSecurityGroupVpc",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:RejectVpcPeeringConnection",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "AllowLocalGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLocalGatewayRoute",
        "ec2:CreateLocalGatewayRouteTableVpcAssociation",
        "ec2:DeleteLocalGatewayRoute",
        "ec2:DeleteLocalGatewayRouteTableVpcAssociation",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLocalGateways",
        "ec2:SearchLocalGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DiscoverBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "s3:ListBucket"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DiscoverFlowLogRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/flow-logs-*"
    },
    {
```

```
      "Sid" : "NetworkmanagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TransitGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptTransitGatewayVpcAttachment",
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:CreateTransitGateway",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:DeleteTransitGateway",
        "ec2:DeleteTransitGatewayRoute",
        "ec2:DeleteTransitGatewayRouteTable",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DisableTransitGatewayRouteTablePropagation",
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:ExportTransitGatewayRoutes",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:ModifyTransitGateway",
        "ec2:ModifyTransitGatewayVpcAttachment",
        "ec2:RejectTransitGatewayVpcAttachment",
        "ec2:ReplaceTransitGatewayRoute",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTransitGatewaySLRCreation",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "transitgateway.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

NetworkSecurityDirectorServiceLinkedRolePolicy

Descrição: Fornece permissões para a função vinculada ao serviço de diretor de segurança de rede AWS Shield para avaliar ambientes específicos.

`NetworkSecurityDirectorServiceLinkedRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 13 de junho de 2025, 20:07 UTC
- Horário editado: 24 de setembro de 2026, 18:17 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/NetworkSecurityDirectorServiceLinkedRolePolicy`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceLevelPermissionNotSupported",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
```

```
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetManagedPrefixListEntries",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "wafv2:ListWebACLs",
        "cloudfront:ListDistributions",
        "cloudfront:ListTagsForResource",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "cloudfront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "classicWaf",
      "Effect" : "Allow",
      "Action" : [
        "waf:ListWebACLs",
        "waf:GetWebACL"
      ],
      "Resource" : [
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*"
      ]
    },
    {
      "Sid" : "wafv2",
```

```
      "Effect" : "Allow",
      "Action" : [
        "wafv2:ListResourcesForWebACL",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:GetRuleGroup",
        "wafv2:DescribeManagedRuleGroup",
        "wafv2:GetWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/webacl/*/*",
        "arn:aws:wafv2:*:*:regional/webacl/*/*",
        "arn:aws:apprunner:*:*:service/*",
        "arn:aws:cognito-idp:*:*:userpool/*",
        "arn:aws:ec2:*:*:verified-access-instance/*"
      ]
    },
    {
      "Sid" : "directconnect",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeVirtualGateways"
      ],
      "Resource" : [
        "arn:aws:directconnect::*:dx-gateway/*",
        "arn:aws:directconnect:*:*:dxcon/*",
        "arn:aws:directconnect:*:*:dxlag/*",
        "arn:aws:directconnect:*:*:dxvif/*"
      ]
    },
    {
      "Sid" : "ec2Get",
      "Effect" : "Allow",
      "Action" : [
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ]
    },
    {
      "Sid" : "networkFirewall",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListFirewalls",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListRuleGroups",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup"
      ],
      "Resource" : [
        "arn:aws:network-firewall:*:*:*/*"
      ]
    },
    {
      "Sid" : "apiGatewayGetAPI",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "AllowOrganizationsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
```

```
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationsAdmins",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "network-security-director.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAccountInformationRead",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetRegionOptStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowConfigRecorderList",
      "Effect" : "Allow",
      "Action" : [
        "config:ListConfigurationRecorders"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowConfigRecorderScopedAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "config:ConfigurationRecorderServicePrincipal" : [
            "network-security-director.amazonaws.com"
          ]
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "DisableNSDPolicyType",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DisablePolicyType"
      ],
      "Resource" : "arn:aws:organizations::*:root/o-*/r-*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : "NETWORK_SECURITY_DIRECTOR_POLICY"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

NetworkSecurityManagerServiceRolePolicy

Descrição: Política de acesso para permitir que a função vinculada ao NetworkSecurityManager serviço realize NetworkSecurityManager-related ações nos NetworkSecurityManager-managed recursos de um cliente Conta da AWS.

`NetworkSecurityManagerServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 18 de agosto de 2026, 18:27 UTC
- Horário editado: 18 de agosto de 2026, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/NetworkSecurityManagerServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LogsGeneral",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "S3LogBucketGeneral",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::aws-waf-logs-*"
    },
    {
      "Sid" : "CloudfrontVpcOriginAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetVpcOrigin"
      ],
      "Resource" : "arn:aws:cloudfront::*:vpcorigin/*"
    },
    {
      "Sid" : "ConfigUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "config:SelectResourceConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeOrganizationUnScoped",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeAccountScoped",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeAccount",
```

```
      "Resource" : "arn:aws:organizations::*:account/o-*/*"
    },
    {
      "Sid" : "DescribeOrganizationUnitScoped",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganizationalUnit",
      "Resource" : "arn:aws:organizations::*:ou/o-*/ou-*"
    },
    {
      "Sid" : "ListDelegatedAdministratorsScoped",
      "Effect" : "Allow",
      "Action" : "organizations:ListDelegatedAdministrators",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "network-security-manager.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LoadBalancerNonMutationApiAccess",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeWebACLAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LoadBalancerGetWebACLScoped",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:GetLoadBalancerWebACL",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "CloudFrontDistributionNonMutationApiAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListTagsForResource"
```

```
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "ApiGatewayStageNonMutationApiAccess",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*"
      ]
    },
    {
      "Sid" : "Wafv2General",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:TagResource",
        "wafv2:ListResourcesForWebACL",
        "wafv2:AssociateWebACL",
        "wafv2:ListTagsForResource",
        "wafv2:UntagResource",
        "wafv2:GetWebACL",
        "wafv2:DisassociateFirewallManager",
        "wafv2:DeleteWebACL",
        "wafv2:DisassociateWebACL",
        "wafv2:ValidateNetworkSecurityManagerWebACLConfiguration",
        "wafv2:ValidateNetworkSecurityManagerRuleConfiguration"
      ],
      "Resource" : "arn:aws:wafv2:*:*:*/webacl/*"
    },
    {
      "Sid" : "Wafv2WebAclAndRuleGroupMutation",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:UpdateWebACL",
        "wafv2:CreateWebACL",
        "wafv2:DeleteFirewallManagerRuleGroups",
        "wafv2:PutFirewallManagerRuleGroups"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*",
        "arn:aws:wafv2:*:*:global/rulegroup/*",
```

```
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/ipset/*",
        "arn:aws:wafv2:*:*:regional/ipset/*",
        "arn:aws:wafv2:*:*:global/regexpatternset/*",
        "arn:aws:wafv2:*:*:regional/regexpatternset/*"
      ]
    },
    {
      "Sid" : "Wafv2Logging",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : "arn:aws:wafv2:*:*:*/webacl/*"
    },
    {
      "Sid" : "Wafv2ListLogging",
      "Effect" : "Allow",
      "Action" : "wafv2:ListLoggingConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "Wafv2ListWebACLs",
      "Effect" : "Allow",
      "Action" : "wafv2:ListWebACLs",
      "Resource" : "*"
    },
    {
      "Sid" : "Wafv2PermissionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutPermissionPolicy",
        "wafv2:GetPermissionPolicy",
        "wafv2:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*"
      ]
    },
```

```
    {
      "Sid" : "Wafv2WebaclDescribe",
      "Effect" : "Allow",
      "Action" : "wafv2:GetWebACLForResource",
      "Resource" : "arn:aws:wafv2:*:*:*/webacl/*"
    },
    {
      "Sid" : "CloudFrontListDistributions",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListDistributions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFrontDistributionMutation",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:DisassociateDistributionWebACL"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "ElbWebAclRemediationScoped",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateWebACLAssociation",
        "elasticloadbalancing:DeleteWebACLAssociation"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "ElbSetWebAcl",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:SetWebACL",
      "Resource" : "*"
    },
    {
      "Sid" : "ApiGatewayWebAclRemediation",
      "Effect" : "Allow",
      "Action" : "apigateway:SetWebACL",
      "Resource" : "arn:aws:apigateway:*::/restapis/*/stages/*"
```

```
    },
    {
      "Sid" : "CognitoWebAclIntegration",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:GetWebACLForResource",
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AppRunnerWebAclIntegration",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:DescribeWebAclForService",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VerifiedAccessWebAclIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AppSyncWebAclIntegration",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetWebACLForResource",
        "appsync:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifyWebAclIntegration",
      "Effect" : "Allow",
      "Action" : [
        "amplify:GetWebACLForResource",
        "amplify:ListResourcesForWebACL"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ShieldGeneral",
      "Effect" : "Allow",
      "Action" : [
        "shield:CreateProtection",
        "shield:DeleteProtection",
        "shield:DescribeProtection",
        "shield:ListProtections",
        "shield:CreateSubscription",
        "shield:DescribeSubscription",
        "shield:GetSubscriptionState",
        "ec2:DescribeAddresses",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ShieldSlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/shield.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "shield.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowConfigRecorderList",
      "Effect" : "Allow",
      "Action" : "config:ListConfigurationRecorders",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutServiceLinkedConfigRecorder",
      "Effect" : "Allow",
      "Action" : "config:PutServiceLinkedConfigurationRecorder",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowConfigRecorderScopedAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:AssociateResourceTypes",
        "config:DisassociateResourceTypes"
      ],
      "Resource" : "arn:aws:config:*:*:configuration-recorder/*"
    },
    {
      "Sid" : "AllowCreateConfigServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowListActionsForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAgentCoreGateway",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:GatewayGetWebACLForResource"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:gateway/*"
    },
    {
      "Sid" : "WafV2LoggingSlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/wafv2.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "wafv2.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

NovaActServiceRolePolicy

Descrição: Esta política permite NovaAct criar e gerenciar os recursos necessários para operar os agentes da Nova Act.

`NovaActServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 26 de novembro de 2025, 16:19 UTC
- Horário editado: 26 de novembro de 2025, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/NovaActServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPublishCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NovaAct"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

OAMFullAccess

Descrição: Fornece acesso total ao CloudWatch Observability Access Manager

`OAMFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `OAMFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de novembro de 2022, 13:38 UTC
- Hora da edição: 27 de novembro de 2022, 13:38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

OAMReadOnlyAccess

Descrição: Fornece acesso somente de leitura ao CloudWatch Observability Access Manager

`OAMReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `OAMReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de novembro de 2022, 13:29 UTC
- Hora da edição: 27 de novembro de 2022, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/OAMReadOnlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:Get*",
        "oam:List*"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

OpensearchIngestionSelfManagedVpcePolicy

Descrição: permite que o Amazon OpenSearch Ingestion descreva recursos de rede e grave métricas de serviço no cloudwatch

`OpensearchIngestionSelfManagedVpcePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 10 de junho de 2024, 19:59 UTC
- Hora da edição: 10 de junho de 2024, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/OpensearchIngestionSelfManagedVpcePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CwPermissionsForOsiNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/OSIS"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

PartnerCentralAccountManagementUserRoleAssociation

Descrição: fornece acesso para associar e dissociar usuários centrais de parceiros com perfis do IAM

`PartnerCentralAccountManagementUserRoleAssociation` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `PartnerCentralAccountManagementUserRoleAssociation` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 10 de novembro de 2023, 2:03 UTC
- Hora da edição: 10 de novembro de 2023, 2:03 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PassPartnerCentralRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/PartnerCentralRoleFor*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "partnercentral-account-management.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "PartnerUserRoleAssociation",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "partnercentral-account-management:AssociatePartnerUser",
        "partnercentral-account-management:DisassociatePartnerUser"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

PartnerCentralIncentiveBenefitManagement

Descrição: A política fornece acesso para gerenciar todos os benefícios de incentivo no AWS Partner Central.

`PartnerCentralIncentiveBenefitManagement` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `PartnerCentralIncentiveBenefitManagement` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 11 de fevereiro de 2026, 16:42 UTC
- Horário editado: 12 de março de 2026, 16:57 UTC

- ARN: `arn:aws:iam::aws:policy/PartnerCentralIncentiveBenefitManagement`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BenefitsManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListBenefits",
        "partnercentral:GetBenefit",
        "partnercentral:CreateBenefitApplication",
        "partnercentral:AmendBenefitApplication",
        "partnercentral:UpdateBenefitApplication",
        "partnercentral:SubmitBenefitApplication",
        "partnercentral:GetBenefitApplication",
        "partnercentral:CancelBenefitApplication",
        "partnercentral:RecallBenefitApplication",
        "partnercentral:ListBenefitApplications",
        "partnercentral:AssociateBenefitApplicationResource",
        "partnercentral:DisassociateBenefitApplicationResource",
        "partnercentral:ListBenefitAllocations",
        "partnercentral:GetBenefitAllocation"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/benefit-application/*",
        "arn:aws:partnercentral:*:*:catalog/*/benefit-allocation/*",
        "arn:aws:partnercentral:*:*:catalog/*/benefit/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
```

```
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerCentralBenefitsTaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/benefit-application/*",
        "arn:aws:partnercentral:*:*:catalog/*/benefit-allocation/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/partner/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AWSPartnerOpportunityAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetAwsOpportunitySummary",
        "partnercentral:GetOpportunity",
        "partnercentral:ListOpportunities"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/opportunity/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "ListingAWSMarketplaceEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceOffersAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Solution/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/OfferSet/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAgreementsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerCentralEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-
files/${aws:PrincipalAccount}/*"
    },
    {
      "Sid" : "PartnerCentralAgentsSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:UseSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        },
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

PowerUserAccess

Descrição: Fornece acesso total aos AWS serviços e recursos, mas não permite o gerenciamento de usuários e grupos.

`PowerUserAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `PowerUserAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:39 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/PowerUserAccess`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "NotAction" : [
        "iam:*",
        "organizations:*",
        "account:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetGovCloudAccountInformation",
        "account:GetPrimaryEmail",
        "account:ListRegions",
        "iam:CreateServiceLinkedRole",
        "iam:DeleteServiceLinkedRole",
        "iam:ListRoles",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

PricingPlanManagerFullAccess

Descrição: Fornece acesso total ao AWS Pricing Plan Manager

`PricingPlanManagerFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `PricingPlanManagerFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 30 de julho de 2026, 16:42 UTC
- Horário editado: 30 de julho de 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/PricingPlanManagerFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ppmglobalactions",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:GetSubscription",
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:CreateSubscription",
        "pricingplanmanager:ApprovePaidSubscription",
        "pricingplanmanager:UpdateSubscription",
        "pricingplanmanager:CancelSubscription",
        "pricingplanmanager:CancelSubscriptionChange",
        "pricingplanmanager:AssociateResourcesToSubscription",
        "pricingplanmanager:DisassociateResourcesFromSubscription",
        "freetier:GetAccountPlanState",
        "cloudwatch:GetMetricData",
        "shield:ListProtections"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

PricingPlanManagerReadonlyAccess

Descrição: Fornece acesso somente para leitura ao AWS Pricing Plan Manager

`PricingPlanManagerReadonlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `PricingPlanManagerReadonlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 30 de julho de 2026, 16:42 UTC
- Horário editado: 30 de julho de 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/PricingPlanManagerReadonlyAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ppmglobalactions",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:GetSubscription"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

QAppsServiceRolePolicy

Descrição: Concede permissões Serviços da AWS e recursos usados ou gerenciados pelo Amazon Q Apps.

`QAppsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 26 de setembro de 2024, 19:22 UTC
- Hora da edição: 26 de setembro de 2024, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QAppsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QAppsPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/QApps"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM

- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

QBusinessQuicksightPluginPolicy

Descrição: Concede permissões ao QBusiness para chamar QuickSight APIs para o plug-in QuickSight

`QBusinessQuicksightPluginPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `QBusinessQuicksightPluginPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de dezembro de 2024, 15:36 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/QBusinessQuicksightPluginPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QBusinessToQuickSightPredictQAResultsInvocation",
      "Effect" : "Allow",
      "Action" : [
```

```
        "quicksight:PredictQAResults"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:topic/*",
        "arn:aws:quicksight:*:*:dashboard/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

QBusinessServiceRolePolicy

Descrição: Concede permissões Serviços da AWS e recursos usados ou gerenciados pela Amazon Q

`QBusinessServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 29 de abril 2024, 16:05 UTC
- Hora da edição: 29 de abril de 2024, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QBusinessServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QBusinessPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/QBusiness"
        }
      }
    },
    {
      "Sid" : "QBusinessCreateLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/qbusiness/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QBusinessDescribeLogGroupsPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QBusinessLogStreamPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/qbusiness/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

Descrição: Política usada pela QuickSight equipe para acessar os dados do cliente produzidos pelo S3 Storage Management Analytics.

`QuickSightAccessForS3StorageManagementAnalyticsReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `QuickSightAccessForS3StorageManagementAnalyticsReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 12 de junho de 2017, 18:18 UTC
- Hora da edição: 08 de outubro de 2019, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::s3-analytics-export-shared-*"
      ]
    },
    {
```

```
      "Action" : [
        "s3:GetAnalyticsConfiguration",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

RDSCloudHsmAuthorizationRole

Descrição: política padrão para o perfil de serviço do Amazon RDS.

`RDSCloudHsmAuthorizationRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `RDSCloudHsmAuthorizationRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 26 de setembro de 2019, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm:DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ReadOnlyAccess

Descrição: Fornece acesso somente para leitura a AWS serviços e recursos.

`ReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:39 UTC
- Horário editado: 24 de setembro de 2026, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

Versão da política

Versão da política: v190 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActionsGroup1",
      "Effect" : "Allow",
      "Action" : [
        "a4b:Get*",
        "a4b:List*",
        "a4b:Search*",
        "access-analyzer:GetAccessPreview",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:GetFindingsStatistics",
        "access-analyzer:GetGeneratedPolicy",
        "access-analyzer:ListAccessPreviewFindings",
        "access-analyzer:ListAccessPreviews",
```

```
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListPolicyGenerations",
        "access-analyzer:ListTagsForResource",
        "access-analyzer:ValidatePolicy",
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:GetGovCloudAccountInformation",
        "account:GetPrimaryEmail",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "acm-pca:Describe*",
        "acm-pca:Get*",
        "acm-pca:List*",
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "acm:SearchCertificates",
        "action-recommendations:ListRecommendedActions",
        "agent-registry:GetDiscoverableRegistryRecord",
        "agent-registry:GetRegistry",
        "agent-registry:GetRegistryRecord",
        "agent-registry:InvokeRegistryMcp",
        "agent-registry:ListDiscoverableRegistryRecords",
        "agent-registry:ListRegistries",
        "agent-registry:ListRegistryRecords",
        "agent-registry:ListTagsForResource",
        "agent-registry:SearchDiscoverableRegistryRecords",
        "aidevops:DescribePrivateConnection",
        "aidevops:DescribeServices",
        "aidevops:GetAccountUsage",
        "aidevops:GetAgentSpace",
        "aidevops:GetAssociation",
        "aidevops:GetBacklogTask",
        "aidevops:GetKnowledgeItem",
        "aidevops:GetOperatorApp",
        "aidevops:GetRecommendation",
        "aidevops:GetService",
        "aidevops:ListAgentSpaces",
        "aidevops:ListAssociations",
        "aidevops:ListBacklogTasks",
```

```
        "aidevops:ListChats",
        "aidevops:ListExecutions",
        "aidevops:ListGoals",
        "aidevops:ListJournalRecords",
        "aidevops:ListKnowledgeItems",
        "aidevops:ListKnowledgeItemVersions",
        "aidevops:ListPendingMessages",
        "aidevops:ListPrivateConnections",
        "aidevops:ListRecommendations",
        "aidevops:ListServices",
        "aidevops:ListTagsForResource",
        "aidevops:ListWebhooks",
        "aidevops:SearchServiceAccessibleResource",
        "aiops:GetEphemeralInvestigationResults",
        "aiops:GetFact",
        "aiops:GetFactVersions",
        "aiops:GetInvestigation",
        "aiops:GetInvestigationEvent",
        "aiops:GetInvestigationGroup",
        "aiops:GetInvestigationResource",
        "aiops:GetReport",
        "aiops:ListFacts",
        "aiops:ListInvestigationEvents",
        "aiops:ListInvestigationGroups",
        "aiops:ListInvestigations",
        "aiops:ValidateInvestigationGroup",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBackendEnvironment",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:GetJob",
        "amplify:GetWebhook",
        "amplify:ListApps",
        "amplify:ListArtifacts",
        "amplify:ListBackendEnvironments",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListJobs",
        "amplify:ListTagsForResource",
        "amplify:ListWebhooks",
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
```

```
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetAccountSettings",
        "aoss:GetPoliciesStats",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "apigateway:GET",
        "apigateway:GetPortal",
        "apigateway:GetPortalProduct",
        "apigateway:GetProductPage",
        "apigateway:GetProductRestEndpointPage",
        "apigateway:GetRoutingRule",
        "apigateway:ListPortalProducts",
        "apigateway:ListPortals",
        "apigateway:ListProductPages",
        "apigateway:ListProductRestEndpointPages",
        "apigateway:ListRoutingRules",
        "apigateway:GetPortalProductSharingPolicy",
        "appconfig:GetApplication",
        "appconfig:GetConfiguration",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtension",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appconfig:GetAccountSettings",
```

```
        "appconfig:GetExperimentDefinition",
        "appconfig:GetExperimentRun",
        "appconfig:GetExtensionAssociation",
        "appconfig:ListExperimentDefinitions",
        "appconfig:ListExperimentRunEvents",
        "appconfig:ListExperimentRuns",
        "appconfig:ListExtensionAssociations",
        "appfabric:GetAppAuthorization",
        "appfabric:GetAppBundle",
        "appfabric:GetIngestion",
        "appfabric:GetIngestionDestination",
        "appfabric:ListAppAuthorizations",
        "appfabric:ListAppBundles",
        "appfabric:ListIngestionDestinations",
        "appfabric:ListIngestions",
        "appfabric:ListTagsForResource",
        "appflow:DescribeConnector",
        "appflow:DescribeConnectorEntity",
        "appflow:DescribeConnectorFields",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeConnectors",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecution",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:DescribeFlows",
        "appflow:ListConnectorEntities",
        "appflow:ListConnectorFields",
        "appflow:ListConnectors",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "application-autoscaling:GetPredictiveScalingForecast",
        "application-autoscaling:ListTagsForResource",
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListAuditFindings",
        "application-signals:ListEntityEvents",
        "application-signals:ListGroupingAttributeDefinitions",
        "application-signals:ListObservedEntities",
        "application-signals:ListServiceDependencies",
        "application-signals:ListServiceDependents",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListServiceLevelObjectives",
```

```
        "application-signals:ListServiceOperations",
        "application-signals:ListServices",
        "application-signals:ListServiceStates",
        "application-signals:ListTagsForResource",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListAssociatedServicesForWebAcl",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListServicesForAutoScalingConfiguration",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:Describe*",
        "appstream:List*",
        "appstudio:GetAccountStatus",
        "appstudio:GetEnablementJobStatus",
        "appsync:Get*",
        "appsync:List*",
        "appsync:EvaluateMappingTemplate",
        "apptest:GetTestCase",
        "apptest:GetTestConfiguration",
        "apptest:GetTestRunStep",
        "apptest:GetTestSuite",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "apptest:ListTestConfigurations",
        "apptest:ListTestRuns",
        "apptest:ListTestRunSteps",
        "apptest:ListTestRunTestCases",
        "apptest:ListTestSuites",
        "aps:DescribeAlertManagerDefinition",
```

```
        "aps:DescribeAnomalyDetector",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration",
        "aps:DescribeResourcePolicy",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeScraperLoggingConfiguration",
        "aps:DescribeWorkspace",
        "aps:DescribeWorkspaceConfiguration",
        "aps:GetAlertManagerSilence",
        "aps:GetAlertManagerStatus",
        "aps:GetDefaultScraperConfiguration",
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:ListAlertManagerAlertGroups",
        "aps:ListAlertManagerAlerts",
        "aps:ListAlertManagerReceivers",
        "aps:ListAlertManagerSilences",
        "aps:ListAlerts",
        "aps:ListAnomalyDetectors",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListRules",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "aps:PreviewAnomalyDetector",
        "aps:QueryMetrics",
        "arc-region-switch:GetPlan",
        "arc-region-switch:GetPlanEvaluationStatus",
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:GetPlanInRegion",
        "arc-region-switch:ListPlanExecutionEvents",
        "arc-region-switch:ListPlanExecutions",
        "arc-region-switch:ListPlans",
        "arc-region-switch:ListPlansInRegion",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListRoute53HealthChecksInRegion",
        "arc-region-switch:ListTagsForResource",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:ListAutoshifts",
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts",
```

```
        "artifact:GetCustomerAgreement",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements",
        "artifact:ListReports",
        "artifact:ListReportVersions",
        "athena:Batch*",
        "athena:Get*",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetAssessmentReportUrl",
        "auditmanager:GetChangeLogs",
        "auditmanager:GetControl",
        "auditmanager:GetDelegations",
        "auditmanager:GetEvidence",
        "auditmanager:GetEvidenceByEvidenceFolder",
        "auditmanager:GetEvidenceFolder",
        "auditmanager:GetEvidenceFoldersByAssessment",
        "auditmanager:GetEvidenceFoldersByAssessmentControl",
        "auditmanager:GetOrganizationAdminAccount",
        "auditmanager:GetServicesInScope",
        "auditmanager:GetSettings",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
        "auditmanager:ListControls",
        "auditmanager:ListKeywordsForDataSource",
        "auditmanager:ListNotifications",
        "auditmanager:ListTagsForResource",
        "auditmanager:ValidateAssessmentReportIntegrity",
        "autoscaling-plans:Describe*",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:Describe*",
        "autoscaling:GetPredictiveScalingForecast",
        "aws-portal:View*",
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway",
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings",
        "backup-gateway:GetVirtualMachine",
```

```
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:Describe*",
        "backup:Get*",
        "backup:List*",
        "batch:Describe*",
        "batch:List*",
        "bedrock-agentcore:GetABTest",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBatchEvaluation",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetBrowserProfile",
        "bedrock-agentcore:GetBrowserSession",
        "bedrock-agentcore:GetCapacityProvider",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetCodeInterpreterSession",
        "bedrock-agentcore:GetConfigurationBundle",
        "bedrock-agentcore:GetConfigurationBundleVersion",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetEvent",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetHarness",
        "bedrock-agentcore:GetHarnessEndpoint",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetMemoryRecord",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetPolicyGeneration",
        "bedrock-agentcore:GetRecommendation",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListAgentRuntimeVersionsByCapacityProvider",
        "bedrock-agentcore:ListCapacityProviders",
        "bedrock-agentcore:ListABTests",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListAgentRuntimeVersions",
```

```
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBatchEvaluations",
        "bedrock-agentcore:ListBrowserProfiles",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListBrowserSessions",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListCodeInterpreterSessions",
        "bedrock-agentcore:ListConfigurationBundles",
        "bedrock-agentcore:ListConfigurationBundleVersions",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListEvents",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListHarnesses",
        "bedrock-agentcore:ListHarnessEndpoints",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListMemoryRecords",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListPolicyGenerationAssets",
        "bedrock-agentcore:ListPolicyGenerations",
        "bedrock-agentcore:ListRecommendations",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock-agentcore:RetrieveMemoryRecords",
        "bedrock-agentcore:GetPolicyEngineSummary",
        "bedrock-agentcore:GetPolicyGenerationSummary",
        "bedrock-agentcore:GetPolicySummary",
        "bedrock-agentcore:ListPolicyEngineSummaries",
        "bedrock-agentcore:ListPolicyGenerationSummaries",
        "bedrock-agentcore:ListPolicySummaries",
        "bedrock-agentcore:GetResourcePolicy",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:GetCustomModel",
        "bedrock:GetDataSource",
        "bedrock:GetEvaluationJob",
        "bedrock:GetFlow",
```

```
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestionJob",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPrompt",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:GetResourcePolicy",
        "bedrock:GetUseCaseForModelAccess",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAgentVersions",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListEnforcedGuardrailsConfiguration",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListFlowVersions",
        "bedrock:ListFoundationModelAgreementOffers",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListIngestionJobs",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListModelInvocationJobs",
        "bedrock:ListPrompts",
        "bedrock:ListProvisionedModelThroughputs",
        "bedrock:AgenticRetrieveStream",
        "bedrock:CheckIngestedDocumentAcl",
        "bedrock:CountTokens",
        "bedrock:GetAccountDataRetention",
        "bedrock:GetAdvancedPromptOptimizationJob",
        "bedrock:GetAgentMemory",
```

```
        "bedrock:GetAsyncInvoke",
        "bedrock:GetAutomatedReasoningPolicy",
        "bedrock:GetAutomatedReasoningPolicyAnnotations",
        "bedrock:GetAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:GetAutomatedReasoningPolicyBuildWorkflowResultAssets",
        "bedrock:GetAutomatedReasoningPolicyNextScenario",
        "bedrock:GetAutomatedReasoningPolicyTestCase",
        "bedrock:GetAutomatedReasoningPolicyTestResult",
        "bedrock:GetBlueprint",
        "bedrock:GetBlueprintOptimizationStatus",
        "bedrock:GetBlueprintRecommendation",
        "bedrock:GetCustomModelDeployment",
        "bedrock:GetDataAutomationLibrary",
        "bedrock:GetDataAutomationLibraryEntity",
        "bedrock:GetDataAutomationLibraryIngestionJob",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataAutomationStatus",
        "bedrock:GetDocumentContent",
        "bedrock:GetExecutionFlowSnapshot",
        "bedrock:GetFlowExecution",
        "bedrock:GetImportedModel",
        "bedrock:GetIngestedDocumentAcl",
        "bedrock:GetInvocationStep",
        "bedrock:GetInvoke",
        "bedrock:GetKnowledgeBaseDocuments",
        "bedrock:GetMarketplaceModelEndpoint",
        "bedrock:GetModelCopyJob",
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:GetCustomizedModel",
        "bedrock-mantle:GetFile",
        "bedrock-mantle:GetFineTuningJob",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:GetProject",
        "bedrock-mantle:GetReservation",
        "bedrock-mantle:ListCustomizedModelAssociations",
        "bedrock-mantle:ListCustomizedModels",
        "bedrock-mantle:ListFiles",
        "bedrock-mantle:ListFineTuningJobs",
        "bedrock-mantle:ListModels",
        "bedrock-mantle:ListProjects",
        "bedrock-mantle:ListReservations",
        "bedrock-mantle:ListTagsForResource",
        "billing:GetBillingData",
```

```
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetBillingView",
        "billing:GetCreditAllocationHistory",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetResourcePolicy",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billingconductor:GetBillingGroupCostReport",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroupCostReports",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListCustomLineItemVersions",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingPlansAssociatedWithPricingRule",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListResourcesAssociatedToCustomLineItem",
        "billingconductor:ListTagsForResource",
        "braket:GetDevice",
        "braket:GetJob",
        "braket:GetQuantumTask",
        "braket:SearchDevices",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "braket:SearchSpendingLimits",
        "budgets:Describe*",
        "budgets:ListTagsForResource",
        "budgets:View*",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:DescribeNotificationSubscription",
        "ce:DescribeReport",
        "ce:GetAnomalies",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:GetApproximateUsageRecords",
        "ce:GetCommitmentPurchaseAnalysis",
```

```
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageComparisons",
        "ce:GetCostAndUsageWithResources",
        "ce:GetCostCategories",
        "ce:GetCostComparisonDrivers",
        "ce:GetCostForecast",
        "ce:GetDimensionValues",
        "ce:GetPreferences",
        "ce:GetReservationCoverage",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetReservationUtilization",
        "ce:GetRightsizingRecommendation",
        "ce:GetSavingsPlanPurchaseRecommendationDetails",
        "ce:GetSavingsPlansCoverage",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "ce:GetSavingsPlansUtilization",
        "ce:GetSavingsPlansUtilizationDetails",
        "ce:GetTags",
        "ce:GetUsageForecast",
        "ce:ListCommitmentPurchaseAnalyses",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:ListCostAllocationTags",
        "ce:ListCostCategoryDefinitions",
        "ce:ListCostCategoryResourceAssociations",
        "ce:ListSavingsPlansPurchaseRecommendationGeneration",
        "ce:ListTagsForResource",
        "chatbot:Describe*",
        "chatbot:Get*",
        "chatbot:List*",
        "chime:Get*",
        "chime:List*",
        "chime:Retrieve*",
        "chime:Search*",
        "chime:Validate*",
        "cleanrooms-ml:GetAudienceGenerationJob",
        "cleanrooms-ml:GetAudienceModel",
        "cleanrooms-ml:GetConfiguredAudienceModel",
        "cleanrooms-ml:GetConfiguredAudienceModelPolicy",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListAudienceExportJobs",
        "cleanrooms-ml:ListAudienceGenerationJobs",
        "cleanrooms-ml:ListAudienceModels",
        "cleanrooms-ml:ListConfiguredAudienceModels",
        "cleanrooms-ml:ListTagsForResource",
```

```
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaborationChangeRequest",
        "cleanrooms:GetCollaborationConfiguredAudienceModelAssociation",
        "cleanrooms:GetCollaborationIdNamespaceAssociation",
        "cleanrooms:GetCollaborationPrivacyBudgetTemplate",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetConfiguredTableAssociationAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:GetProtectedJob",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationChangeRequests",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborationIdNamespaceAssociations",
        "cleanrooms:ListCollaborationPrivacyBudgets",
        "cleanrooms:ListCollaborationPrivacyBudgetTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredAudienceModelAssociations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgets",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListProtectedJobs",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
```

```
        "cleanrooms:ListTagsForResource",
        "cleanrooms:PreviewPrivacyImpact",
        "cloud9:Describe*",
        "cloud9:List*",
        "clouddirectory:BatchRead",
        "clouddirectory:Get*",
        "clouddirectory:List*",
        "clouddirectory:LookupPolicy",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:Describe*",
        "cloudformation:Detect*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudhsm:Describe*",
        "cloudhsm:GetResourcePolicy",
        "cloudhsm:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:Describe*",
        "cloudtrail:Get*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GenerateQueryResultsSummary",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackage",
        "codeartifact:DescribePackageVersion",
        "codeartifact:DescribeRepository",
        "codeartifact:GetAuthorizationToken",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetPackageVersionAsset",
        "codeartifact:GetPackageVersionReadme",
        "codeartifact:GetRepositoryEndpoint",
```

```
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersionAssets",
        "codeartifact:ListPackageVersionDependencies",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListRepositoriesInDomain",
        "codeartifact:ListTagsForResource",
        "codeartifact:ReadFromRepository",
        "codebuild:BatchGet*",
        "codebuild:DescribeCodeCoverages",
        "codebuild:DescribeTestCases",
        "codebuild:List*",
        "codecatalyst:GetBillingAuthorization",
        "codecatalyst:GetConnection",
        "codecatalyst:GetPendingConnection",
        "codecatalyst:ListConnections",
        "codecatalyst:ListIamRolesForConnection",
        "codecatalyst:ListTagsForResource",
        "codecommit:BatchGet*",
        "codecommit:Describe*",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:List*",
        "codeconnections:GetConnection",
        "codeconnections:GetHost",
        "codeconnections:GetRepositoryLink",
        "codeconnections:GetRepositorySyncStatus",
        "codeconnections:GetResourceSyncStatus",
        "codeconnections:GetSyncConfiguration",
        "codeconnections:ListConnections",
        "codeconnections:ListHosts",
        "codeconnections:ListRepositoryLinks",
        "codeconnections:ListRepositorySyncDefinitions",
        "codeconnections:ListSyncConfigurations",
        "codeconnections:ListTagsForResource",
        "codedeploy:BatchGet*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "codeguru-reviewer:Describe*",
```

```
        "codeguru-reviewer:Get*",
        "codeguru-reviewer:List*",
        "codepipeline:Get*",
        "codepipeline:List*",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetRepositorySyncStatus",
        "codestar-connections:GetResourceSyncStatus",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:ListConnections",
        "codestar-connections:ListHosts",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListRepositorySyncDefinitions",
        "codestar-connections:ListSyncConfigurations",
        "codestar-connections:ListTagsForResource",
        "codestar-notifications:describeNotificationRule",
        "codestar-notifications:listEventTypes",
        "codestar-notifications:listNotificationRules",
        "codestar-notifications:listTagsForResource",
        "codestar-notifications:ListTargets",
        "codestar:Describe*",
        "codestar:Get*",
        "codestar:List*",
        "codestar:Verify*",
        "codewhisperer:ListProfiles",
        "cognito-identity:Describe*",
        "cognito-identity:GetCredentialsForIdentity",
        "cognito-identity:GetIdentityPoolAnalytics",
        "cognito-identity:GetIdentityPoolDailyAnalytics",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetIdentityProviderDailyAnalytics",
        "cognito-identity:GetOpenIdToken",
        "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
        "cognito-identity:List*",
        "cognito-identity:Lookup*",
        "cognito-idp:AdminGet*",
        "cognito-idp:AdminList*",
        "cognito-idp:Describe*",
        "cognito-idp:Get*",
        "cognito-idp:List*",
        "cognito-sync:Describe*",
        "cognito-sync:Get*",
        "cognito-sync:List*",
```

```
        "cognito-sync:QueryRecords",
        "comprehend:BatchDetect*",
        "comprehend:Classify*",
        "comprehend:Contains*",
        "comprehend:Describe*",
        "comprehend:Detect*",
        "comprehend:List*",
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetIdleRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:GetRDSDatabaseRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetRecommendationSummaries",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:Describe*",
        "connect:GetContactAttributes",
        "connect:GetCurrentMetricData",
        "connect:GetCurrentUserData",
        "connect:GetFederationToken",
        "connect:GetMetricData",
        "connect:GetMetricDataV2",
        "connect:GetTaskTemplate",
        "connect:GetTrafficDistribution",
        "connect:List*",
        "consoleapp:GetDeviceIdentity",
        "consoleapp:ListDeviceIdentities",
```

```
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "controlcatalog:GetControl",
        "controlcatalog:ListCommonControls",
        "controlcatalog:ListControlMappings",
        "controlcatalog:ListControls",
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListEfficiencyMetrics",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeJobRun",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobRuns",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
        "dataexchange:Get*",
        "dataexchange:List*",
        "datapipeline:Describe*",
        "datapipeline:EvaluateExpression",
        "datapipeline:Get*",
        "datapipeline:List*",
        "datapipeline:QueryObjects",
        "datapipeline:Validate*",
        "datasync:Describe*",
```

```
        "datasync:List*",
        "datazone:GetAsset",
        "datazone:GetAssetType",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetDomainSharingPolicy",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetLineageNode",
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
        "datazone:GetProject",
        "datazone:GetProjectProfile",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetRevisions",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDomains",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
```

```
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjectProfiles",
        "datazone:ListProjects",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptions",
        "datazone:ListSubscriptionTargets",
        "datazone:ListTagsForResource",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "dax:BatchGetItem",
        "dax:Describe*",
        "dax:GetItem",
        "dax:ListTags",
        "dax:Query",
        "dax:Scan",
        "deadline:BatchGetJobEntity",
        "deadline:GetApplicationVersion",
        "deadline:GetBudget",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetJob",
        "deadline:GetLicenseEndpoint",
        "deadline:GetLimit",
        "deadline:GetMonitor",
        "deadline:GetMonitorSettings",
        "deadline:GetQueue",
        "deadline:GetQueueLimitAssociation",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetSessionsStatisticsAggregation",
        "deadline:GetStep",
        "deadline:GetStorageProfile",
```

```
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:GetVolume",
        "deadline:GetWorker",
        "deadline:ListAvailableMeteredProducts",
        "deadline:ListBudgets",
        "deadline:ListFarmMembers",
        "deadline:ListFarms",
        "deadline:ListFleetMembers",
        "deadline:ListFleets",
        "deadline:ListJobMembers",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListJobs",
        "deadline:ListLicenseEndpoints",
        "deadline:ListLimits",
        "deadline:ListMeteredProducts",
        "deadline:ListMonitors",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListQueueLimitAssociations",
        "deadline:ListQueueMembers",
        "deadline:ListQueues",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListSessionsForWorker",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfiles",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTagsForResource",
        "deadline:ListTasks",
        "deadline:ListVolumes",
        "deadline:ListWorkers",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks",
        "deadline:SearchWorkers",
        "deepcomposer:GetComposition",
        "deepcomposer:GetModel",
        "deepcomposer:GetSampleModel",
        "deepcomposer:ListCompositions",
        "deepcomposer:ListModels",
        "deepcomposer:ListSampleModels",
```

```
        "deepcomposer:ListTrainingTopics",
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:Get*",
        "detective:List*",
        "detective:SearchGraph",
        "devicefarm:Get*",
        "devicefarm:List*",
        "devops-guru:DescribeAccountHealth",
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeResourceCollectionHealth",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetCostEstimation",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListAnomaliesForInsight",
        "devops-guru:ListAnomalousLogGroups",
        "devops-guru:ListEvents",
        "devops-guru:ListInsights",
        "devops-guru:ListMonitoredResources",
        "devops-guru:ListNotificationChannels",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:ListRecommendations",
        "devops-guru:SearchInsights",
        "devops-guru:StartCostEstimation",
        "directconnect:Describe*",
        "directconnect:ListVirtualInterfaceRoutes",
        "directconnect:ListVirtualInterfaceTestHistory",
        "directconnect:GetResiliencyGroup",
        "directconnect:ListResiliencyGroupAssociations",
        "directconnect:ListResiliencyGroups",
        "discovery:Describe*",
        "discovery:Get*",
        "discovery:List*",
        "dlm:Get*",
        "dlm:ListTagsForResource",
        "dms:Describe*",
        "dms:List*",
```

```
        "dms:Test*",
        "docdb-elastic:GetCluster",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:ListPendingMaintenanceActions",
        "docdb-elastic:ListTagsForResource",
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeLaunchConfigurationTemplates",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceNetworks",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListLaunchActions",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "dsql:GetCluster",
        "dsql:GetClusterPolicy",
        "dsql:GetStream",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListStreams",
        "dsql:ListTagsForResource",
        "dynamodb:BatchGet*",
        "dynamodb:Describe*",
        "dynamodb:Get*",
        "dynamodb:List*",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:ReadDataForReplication",
        "dynamodb:SearchVectors",
        "ec2:Describe*",
```

```
        "ec2:DescribeInstanceImageMetadata",
        "ec2:Get*",
        "ec2:ListImagesInRecycleBin",
        "ec2:ListSnapshotsInRecycleBin",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:ListVolumesInRecycleBin",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2messages:Get*",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetAuthorizationToken",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchCheck*",
        "ecr:BatchGet*",
        "ecr:Describe*",
        "ecr:Get*",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:GetTaskProtection",
        "ecs:List*",
        "eks:AccessKubernetesApi",
        "eks:Describe*",
        "eks:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:Request*",
        "elasticbeanstalk:Retrieve*",
        "elasticbeanstalk:Validate*",
        "elasticfilesystem:Describe*",
        "elasticfilesystem:ListTagsForResource",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:List*",
```

```
        "elasticmapreduce:View*",
        "elastictranscoder:List*",
        "elastictranscoder:Read*",
        "elemental-appliances-software:Get*",
        "elemental-appliances-software:List*",
        "elemental-inference:ExportDictionaryEntries",
        "elemental-inference:GetDictionary",
        "elemental-inference:GetFeed",
        "elemental-inference:ListDictionaries",
        "elemental-inference:ListFeeds",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "emr-serverless:ListTagsForResource",
        "es:Describe*",
        "es:ESHttpGet",
        "es:ESHttpHead",
        "es:Get*",
        "es:List*",
        "events:Describe*",
        "events:List*",
        "events:Test*",
        "evidently:GetExperiment",
        "evidently:GetExperimentResults",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegmentReferences",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
```

```
        "evidently:TestSegmentPattern",
        "firehose:Describe*",
        "firehose:List*",
        "fis:GetAction",
        "fis:GetExperiment",
        "fis:GetExperimentTargetAccountConfiguration",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:GetTargetResourceType",
        "fis:ListActions",
        "fis:ListExperimentResolvedTargets",
        "fis:ListExperiments",
        "fis:ListExperimentTargetAccountConfigurations",
        "fis:ListExperimentTemplates",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fis:ListTargetResourceTypes",
        "fms:GetAdminAccount",
        "fms:GetAdminScope",
        "fms:GetAppsList",
        "fms:GetComplianceDetail",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:GetProtectionStatus",
        "fms:GetProtocolsList",
        "fms:GetViolationDetails",
        "fms:ListAppsLists",
        "fms:ListComplianceStatus",
        "fms:ListMemberAccounts",
        "fms:ListPolicies",
        "fms:ListProtocolsLists",
        "fms:ListTagsForResource",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeExplainability",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribeMonitor",
        "forecast:DescribePredictor",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:DescribeWhatIfAnalysis",
```

```
        "forecast:DescribeWhatIfForecast",
        "forecast:DescribeWhatIfForecastExport",
        "forecast:GetAccuracyMetrics",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasetImportJobs",
        "forecast:ListDatasets",
        "forecast:ListExplainabilities",
        "forecast:ListExplainabilityExports",
        "forecast:ListForecastExportJobs",
        "forecast:ListForecasts",
        "forecast:ListMonitorEvaluations",
        "forecast:ListMonitors",
        "forecast:ListPredictorBacktestExportJobs",
        "forecast:ListPredictors",
        "forecast:ListWhatIfAnalyses",
        "forecast:ListWhatIfForecastExports",
        "forecast:ListWhatIfForecasts",
        "forecast:QueryForecast",
        "forecast:QueryWhatIfForecast",
        "frauddetector:BatchGetVariable",
        "frauddetector:DescribeDetector",
        "frauddetector:DescribeModelVersions",
        "frauddetector:GetBatchImportJobs",
        "frauddetector:GetBatchPredictionJobs",
        "frauddetector:GetDeleteEventsByEventTypeStatus",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEvent",
        "frauddetector:GetEventPredictionMetadata",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetKMSEncryptionKey",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModels",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListEventPredictions",
        "frauddetector:ListTagsForResource",
        "freertos:Describe*",
```

```
        "freertos:List*",
        "freetier:GetAccountActivity",
        "freetier:GetAccountPlanState",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:ListAccountActivities",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:Describe*",
        "gamelift:Get*",
        "gamelift:List*",
        "gamelift:ResolveAlias",
        "gamelift:Search*",
        "gameliftstreams:GetApplication",
        "gameliftstreams:GetStreamGroup",
        "gameliftstreams:ListApplications",
        "gameliftstreams:ListStreamGroups",
        "gameliftstreams:ListStreamSessions",
        "gameliftstreams:ListStreamSessionsByAccount",
        "gameliftstreams:ListTagsForResource",
        "gameliftstreams:GetStreamUrl",
        "gameliftstreams:ListApplicationShaderCaches",
        "gameliftstreams:ListStreamUrls",
        "glacier:Describe*",
        "glacier:Get*",
        "glacier:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:BatchGetCrawlers",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:BatchGetTriggers",
        "glue:BatchGetWorkflows",
        "glue:CheckSchemaVersionValidity",
        "glue:GetCatalog",
        "glue:GetCatalogImportStatus",
        "glue:GetCatalogs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlerMetrics",
        "glue:GetCrawlers",
```

```
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDataflowGraph",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobBookmark",
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:GetJobs",
        "glue:GetMapping",
        "glue:GetMLTaskRun",
        "glue:GetMLTaskRuns",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetPlan",
        "glue:GetRegistry",
        "glue:GetResourcePolicy",
        "glue:GetSchema",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetTriggers",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions",
        "glue:GetWorkflow",
        "glue:GetWorkflowRun",
        "glue:GetWorkflowRunProperties",
        "glue:GetWorkflowRuns",
        "glue:ListCrawlers",
```

```
        "glue:ListCrawls",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListSchemas",
        "glue:ListSchemaVersions",
        "glue:ListSessions",
        "glue:ListStatements",
        "glue:ListTableOptimizerRuns",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "glue:QuerySchemaVersionMetadata",
        "glue:SearchTables",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListPermissions",
        "grafana:ListTagsForResource",
        "grafana:ListVersions",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:Get*",
        "greengrass:List*",
        "groundstation:DescribeContactVersion",
        "groundstation:DescribeEphemeris",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMinuteUsage",
        "groundstation:GetMissionProfile",
        "groundstation:GetSatellite",
        "groundstation:ListAntennas",
        "groundstation:ListConfigs",
        "groundstation:ListContacts",
        "groundstation:ListContactVersions",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListEphemerides",
        "groundstation:ListGroundStationReservations",
        "groundstation:ListGroundStations",
        "groundstation:ListMissionProfiles",
        "groundstation:ListSatellites",
        "groundstation:ListTagsForResource",
        "groundstation:DescribeContact",
        "guardduty:Describe*",
```

```
        "guardduty:Get*",
        "guardduty:List*",
        "health:Describe*",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:GetCapabilities",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListFHIRExportJobs",
        "healthlake:ListFHIRImportJobs",
        "healthlake:ListTagsForResource",
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost",
        "iam:Generate*",
        "iam:Get*",
        "iam:List*",
        "iam:Simulate*",
        "identity-sync:GetSyncProfile",
        "identity-sync:GetSyncTarget",
        "identity-sync:ListSyncFilters",
        "identitystore-auth:BatchGetSession",
        "identitystore-auth:ListSessions",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetGroupMembershipId",
        "identitystore:GetUserId",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
        "imagebuilder:Get*",
        "imagebuilder:List*",
        "importexport:Get*",
        "importexport:List*",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetCodeSnippet",
```

```
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:BatchGetMemberEc2DeepInspectionStatus",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetCisScanReport",
        "inspector2:GetConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetEc2DeepInspectionConfiguration",
        "inspector2:GetEncryptionKey",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:GetSbomExport",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCisScanConfigurations",
        "inspector2:ListCisScans",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListMembers",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "inspector2:SearchVulnerabilities",
        "inspector2:ListConnectors",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "interconnect:DescribeConnectionProposal",
        "interconnect:GetConnection",
        "interconnect:GetEnvironment",
        "interconnect:ListAttachPoints",
        "interconnect:ListTagsForResource",
        "interconnect:ListEnvironments",
        "interconnect:ListConnections",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "iot:Describe*",
        "iot:Get*",
```

```
        "iot:List*",
        "iot1click:DescribeDevice",
        "iot1click:DescribePlacement",
        "iot1click:DescribeProject",
        "iot1click:GetDeviceMethods",
        "iot1click:GetDevicesInPlacement",
        "iot1click:ListDeviceEvents",
        "iot1click:ListDevices",
        "iot1click:ListPlacements",
        "iot1click:ListProjects",
        "iot1click:ListTagsForResource",
        "iotanalytics:Describe*",
        "iotanalytics:Get*",
        "iotanalytics:List*",
        "iotanalytics:SampleChannelData",
        "iotevents:DescribeAlarm",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetector",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:DescribeLoggingOptions",
        "iotevents:ListAlarmModels",
        "iotevents:ListAlarmModelVersions",
        "iotevents:ListAlarms",
        "iotevents:ListDetectorModels",
        "iotevents:ListDetectorModelVersions",
        "iotevents:ListDetectors",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetLoggingOptions",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetRegisterAccountStatus",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:GetVehicleStatus",
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
```

```
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListFleetsForVehicle",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotfleetwise:ListVehiclesInFleet",
        "iotsitewise:Describe*",
        "iotsitewise:Get*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetEventConfigurationByResourceTypes",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetLogLevelsByResourceTypes",
        "iotwireless:GetMetricConfiguration",
        "iotwireless:GetMetrics",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetMulticastGroupSession",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetPartnerAccount",
        "iotwireless:GetPosition",
        "iotwireless:GetPositionConfiguration",
        "iotwireless:GetPositionEstimate",
        "iotwireless:GetResourceEventConfiguration",
        "iotwireless:GetResourceLogLevel",
        "iotwireless:GetResourcePosition",
        "iotwireless:GetServiceEndpoint",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessDeviceStatistics",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayCertificate",
        "iotwireless:GetWirelessGatewayFirmwareInformation",
        "iotwireless:GetWirelessGatewayStatistics",
        "iotwireless:GetWirelessGatewayTask",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListDevicesForWirelessDeviceImportTask",
        "iotwireless:ListEventConfigurations",
```

```
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListMulticastGroupsByFuotaTask",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListPositionConfigurations",
        "iotwireless:ListQueuedMessages",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetIngestConfiguration",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetPublicKey",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetStorageConfiguration",
        "ivs:GetStream",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListParticipantEvents",
        "ivs:ListParticipants",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStageSessions",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
```

```
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyActionsGroup2",
      "Effect" : "Allow",
      "Action" : [
        "kafka:Describe*",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:Get*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
        "kafka:ListClusterOperations",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurationRevisions",
        "kafka:ListConfigurations",
        "kafka:ListKafkaVersions",
        "kafka:ListNodes",
        "kafka:ListTagsForResource",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra:BatchGetDocumentStatus",
        "kendra:DescribeDataSource",
        "kendra:DescribeExperience",
        "kendra:DescribeFaq",
        "kendra:DescribeIndex",
        "kendra:DescribePrincipalMapping",
        "kendra:DescribeQuerySuggestionsBlockList",
```

```
        "kendra:DescribeQuerySuggestionsConfig",
        "kendra:DescribeThesaurus",
        "kendra:GetQuerySuggestions",
        "kendra:GetSnapshots",
        "kendra:ListDataSources",
        "kendra:ListDataSourceSyncJobs",
        "kendra:ListEntityPersonas",
        "kendra:ListExperienceEntities",
        "kendra:ListExperiences",
        "kendra:ListFaqs",
        "kendra:ListGroupsOlderThanOrderingId",
        "kendra:ListIndices",
        "kendra:ListQuerySuggestionsBlockLists",
        "kendra:ListTagsForResource",
        "kendra:ListThesauri",
        "kendra:Query",
        "kinesis:Describe*",
        "kinesis:Get*",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:Discover*",
        "kinesisanalytics:Get*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kinesisvideo:Get*",
        "kinesisvideo:List*",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetEffectivePermissionsForPath",
        "lakeformation:GetLfTag",
        "lakeformation:GetResourceLfTags",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListLfTags",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListTableStorageOptimizers",
        "lakeformation:SearchDatabasesByLfTags",
        "lakeformation:SearchTablesByLfTags",
        "lambda:Get*",
        "lambda:List*",
```

```
        "launchwizard:DescribeAdditionalNode",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:DescribeProvisioningEvents",
        "launchwizard:DescribeSettingsSet",
        "launchwizard:GetDeployment",
        "launchwizard:GetInfrastructureSuggestion",
        "launchwizard:GetIpAddress",
        "launchwizard:GetResourceCostEstimate",
        "launchwizard:GetResourceRecommendation",
        "launchwizard:GetSettingsSet",
        "launchwizard:GetWorkload",
        "launchwizard:GetWorkloadAsset",
        "launchwizard:GetWorkloadAssets",
        "launchwizard:GetWorkloadDeploymentPattern",
        "launchwizard:ListAdditionalNodes",
        "launchwizard:ListAllowedResources",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListProvisionedApps",
        "launchwizard:ListResourceCostEstimates",
        "launchwizard:ListSettingsSets",
        "launchwizard:ListTagsForResource",
        "launchwizard:ListWorkloadDeploymentOptions",
        "launchwizard:ListWorkloadDeploymentPatterns",
        "launchwizard:ListWorkloads",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
        "lex:DescribeBotReplica",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:Get*",
        "lex:ListBotAliases",
        "lex:ListBotAliasReplicas",
        "lex:ListBotChannels",
        "lex:ListBotLocales",
        "lex:ListBotReplicas",
        "lex:ListBots",
```

```
        "lex:ListBotVersionReplicas",
        "lex:ListBotVersions",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
        "lex:ListIntents",
        "lex:ListSlots",
        "lex:ListSlotTypes",
        "lex:ListTagsForResource",
        "license-manager:Get*",
        "license-manager:List*",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetAutoSnapshots",
        "lightsail:GetBlueprints",
        "lightsail:GetBucketAccessKeys",
        "lightsail:GetBucketBundles",
        "lightsail:GetBucketMetricData",
        "lightsail:GetBuckets",
        "lightsail:GetBundles",
        "lightsail:GetCertificates",
        "lightsail:GetCloudFormationStackRecords",
        "lightsail:GetContainerAPIMetadata",
        "lightsail:GetContainerImages",
        "lightsail:GetContainerServiceDeployments",
        "lightsail:GetContainerServiceMetricData",
        "lightsail:GetContainerServicePowers",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributionBundles",
        "lightsail:GetDistributionLatestCacheReset",
        "lightsail:GetDistributionMetricData",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetExportSnapshotRecords",
        "lightsail:GetInstance",
        "lightsail:GetInstanceMetricData",
        "lightsail:GetInstancePortStates",
        "lightsail:GetInstances",
```

```
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstanceState",
        "lightsail:GetKeyPair",
        "lightsail:GetKeyPairs",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancerMetricData",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperation",
        "lightsail:GetOperations",
        "lightsail:GetOperationsForResource",
        "lightsail:GetRegions",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseBlueprints",
        "lightsail:GetRelationalDatabaseBundles",
        "lightsail:GetRelationalDatabaseEvents",
        "lightsail:GetRelationalDatabaseLogEvents",
        "lightsail:GetRelationalDatabaseLogStreams",
        "lightsail:GetRelationalDatabaseMetricData",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "lightsail:Is*",
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:Get*",
        "logs:ListAggregateLogGroupSummaries",
        "logs:ListAnomalies",
        "logs:ListEntitiesForLogGroup",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListLogGroupsForEntity",
        "logs:ListLogGroupsForQuery",
        "logs:ListScheduledQueries",
        "logs:ListSourcesForS3TableIntegration",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "logs:StartLiveTail",
        "logs:StartQuery",
```

```
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "lookoutequipment:DescribeDataIngestionJob",
        "lookoutequipment:DescribeDataset",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:DescribeLabel",
        "lookoutequipment:DescribeLabelGroup",
        "lookoutequipment:DescribeModel",
        "lookoutequipment:DescribeModelVersion",
        "lookoutequipment:DescribeResourcePolicy",
        "lookoutequipment:DescribeRetrainingScheduler",
        "lookoutequipment:ListDataIngestionJobs",
        "lookoutequipment:ListDatasets",
        "lookoutequipment:ListInferenceEvents",
        "lookoutequipment:ListInferenceExecutions",
        "lookoutequipment:ListInferenceSchedulers",
        "lookoutequipment:ListLabelGroups",
        "lookoutequipment:ListLabels",
        "lookoutequipment:ListModels",
        "lookoutequipment:ListModelVersions",
        "lookoutequipment:ListRetrainingSchedulers",
        "lookoutequipment:ListSensorStatistics",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:Describe*",
        "lookoutmetrics:Get*",
        "lookoutmetrics:List*",
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModelPackagingJobs",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "m2:GetApplication",
        "m2:GetApplicationVersion",
        "m2:GetBatchJobExecution",
        "m2:GetDataSetDetails",
        "m2:GetDataSetImportTask",
        "m2:GetDeployment",
        "m2:GetEnvironment",
        "m2:ListApplications",
```

```
        "m2:ListApplicationVersions",
        "m2:ListBatchJobDefinitions",
        "m2:ListBatchJobExecutions",
        "m2:ListDataSetImportHistory",
        "m2:ListDataSets",
        "m2:ListDeployments",
        "m2:ListEngineVersions",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:Describe*",
        "machinelearning:Get*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:DescribeBuckets",
        "macie2:DescribeClassificationJob",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAdministratorAccount",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetBucketStatistics",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetClassificationScope",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindings",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetFindingStatistics",
        "macie2:GetInvitationsCount",
        "macie2:GetMacieSession",
        "macie2:GetMember",
        "macie2:GetResourceProfile",
        "macie2:GetRevealConfiguration",
        "macie2:GetSensitiveDataOccurrencesAvailability",
        "macie2:GetSensitivityInspectionTemplate",
        "macie2:GetUsageStatistics",
        "macie2:GetUsageTotals",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListClassificationJobs",
        "macie2:ListClassificationScopes",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindings",
        "macie2:ListFindingsFilters",
        "macie2:ListInvitations",
        "macie2:ListMembers",
```

```
        "macie2:ListOrganizationAdminAccounts",
        "macie2:ListResourceProfileArtifacts",
        "macie2:ListResourceProfileDetections",
        "macie2:ListSensitivityInspectionTemplates",
        "macie2:ListTagsForResource",
        "macie2:SearchResources",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:GetProposal",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNetworks",
        "managedblockchain:ListNodes",
        "managedblockchain:ListProposals",
        "managedblockchain:ListProposalVotes",
        "managedblockchain:ListTagsForResource",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeFlowSourceMetadata",
        "mediaconnect:DescribeFlowSourceThumbnail",
        "mediaconnect:DescribeGateway",
        "mediaconnect:DescribeGatewayInstance",
        "mediaconnect:DescribeOffering",
        "mediaconnect:DescribeReservation",
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:GetRouterInput",
        "mediaconnect:GetRouterNetworkInterface",
        "mediaconnect:GetRouterOutput",
        "mediaconnect:ListBridges",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGatewayInstances",
        "mediaconnect:ListGateways",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:ListRouterInputs",
        "mediaconnect:ListRouterNetworkInterfaces",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListTagsForResource",
        "mediaconvert:DescribeEndpoints",
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:Probe",
        "mediaconvert:SearchJobs",
```

```
        "medialive:DescribeAccountConfiguration",
        "medialive:DescribeChannel",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeCluster",
        "medialive:DescribeInput",
        "medialive:DescribeInputDevice",
        "medialive:DescribeInputDeviceThumbnail",
        "medialive:DescribeInputSecurityGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeNetwork",
        "medialive:DescribeOffering",
        "medialive:DescribeReservation",
        "medialive:DescribeSchedule",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:ListChannels",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListInputDevices",
        "medialive:ListInputDeviceTransfers",
        "medialive:ListInputs",
        "medialive:ListInputSecurityGroups",
        "medialive:ListMultiplexes",
        "medialive:ListMultiplexPrograms",
        "medialive:ListOfferings",
        "medialive:ListReservations",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetHeadObject",
        "mediapackagev2:GetObject",
        "mediapackagev2:GetOriginEndpoint",
```

```
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediapackagev2:ListTagsForResource",
        "mediastore:DescribeContainer",
        "mediastore:DescribeObject",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:GetLifecyclePolicy",
        "mediastore:GetMetricPolicy",
        "mediastore:GetObject",
        "mediastore:ListContainers",
        "mediastore:ListItems",
        "mediastore:ListTagsForResource",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeEngineVersions",
        "memorydb:DescribeEvents",
        "memorydb:DescribeMultiRegionClusters",
        "memorydb:DescribeMultiRegionParameterGroups",
        "memorydb:DescribeMultiRegionParameters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeReservedNodes",
        "memorydb:DescribeReservedNodesOfferings",
        "memorydb:DescribeServiceUpdates",
        "memorydb:DescribeSnapshots",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListAllowedMultiRegionClusterUpdates",
        "memorydb:ListAllowedNodeTypeUpdates",
        "memorydb:ListTags",
        "mgh:Describe*",
        "mgh:GetHomeRegion",
        "mgh:List*",
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:DescribeSourceServers",
        "mgn:DescribeVcenterClients",
        "mgn:GetLaunchConfiguration",
        "mgn:GetReplicationConfiguration",
```

```
        "mgn:ListApplications",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListWaves",
        "mobileanalytics:Get*",
        "mobiletargeting:Get*",
        "mobiletargeting:List*",
        "monitron:GetProject",
        "monitron:GetProjectAdminUser",
        "monitron:ListProjects",
        "monitron:ListTagsForResource",
        "mpa:GetApprovalTeam",
        "mpa:GetIdentitySource",
        "mpa:GetPolicyVersion",
        "mpa:GetResourcePolicy",
        "mpa:GetSession",
        "mpa:ListApprovalTeams",
        "mpa:ListIdentitySources",
        "mpa:ListPolicies",
        "mpa:ListPolicyVersions",
        "mpa:ListResourcePolicies",
        "mpa:ListSessions",
        "mpa:ListTagsForResource",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeProxy",
        "network-firewall:DescribeProxyConfiguration",
        "network-firewall:DescribeProxyRule",
        "network-firewall:DescribeProxyRuleGroup",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListProxies",
        "network-firewall:ListProxyConfigurations",
        "network-firewall:ListProxyRuleGroups",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
```

```
        "networkflowmonitor:GetMonitor",
        "networkflowmonitor:GetScope",
        "networkflowmonitor:ListMonitors",
        "networkflowmonitor:ListScopes",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnections",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetConnectPeerAssociations",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkChangeEvents",
        "networkmanager:GetCoreNetworkChangeSet",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetNetworkResourceCounts",
        "networkmanager:GetNetworkResourceRelationships",
        "networkmanager:GetNetworkResources",
        "networkmanager:GetNetworkRoutes",
        "networkmanager:GetNetworkTelemetry",
        "networkmanager:GetResourcePolicy",
        "networkmanager:GetRouteAnalysis",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayConnectPeerAssociations",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachmentRoutingPolicyAssociations",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworkPolicyVersions",
        "networkmanager:ListCoreNetworkPrefixListAssociations",
        "networkmanager:ListCoreNetworkRoutingInformation",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "networkmonitor:GetMonitor",
        "networkmonitor:GetProbe",
        "networkmonitor:ListMonitors",
        "networkmonitor:ListTagsForResource",
```

```
        "nimble:GetEula",
        "nimble:GetFeatureMap",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileMember",
        "nimble:GetStreamingImage",
        "nimble:GetStreamingSession",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:GetStudioMember",
        "nimble:ListEulaAcceptances",
        "nimble:ListEulas",
        "nimble:ListLaunchProfileMembers",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStreamingSessions",
        "nimble:ListStudioComponents",
        "nimble:ListStudioMembers",
        "nimble:ListStudios",
        "nimble:ListTagsForResource",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:ListTagsForResource",
        "notifications:GetEventRule",
        "notifications:GetFeatureOptInStatus",
        "notifications:GetManagedNotificationChildEvent",
        "notifications:GetManagedNotificationConfiguration",
        "notifications:GetManagedNotificationEvent",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:GetNotificationsAccessForOrganization",
        "notifications:List*",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListAttachedLinks",
        "oam:ListLinks",
        "oam:ListSinks",
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
```

```
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "omics:Get*",
        "omics:List*",
        "one:GetDeviceConfigurationTemplate",
        "one:GetDeviceInstance",
        "one:GetDeviceInstanceConfiguration",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceConfigurationTemplates",
        "one:ListDeviceInstances",
        "one:ListSites",
        "one:ListUsers",
        "opsworks-cm:Describe*",
        "opsworks-cm:List*",
        "opsworks:Describe*",
        "opsworks:Get*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:GetPipelineBlueprint",
        "osis:GetPipelineChangeProgress",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "outposts:Get*",
        "outposts:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:GetPublicKeyCertificate",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
```

```
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentInstruments",
        "payments:ListPaymentPreferences",
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListChallengeMetadata",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "personalize:Describe*",
        "personalize:Get*",
        "personalize:List*",
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "polly:Describe*",
        "polly:Get*",
```

```
        "polly:List*",
        "polly:SynthesizeSpeech",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetPriceListFileUrl",
        "pricing:GetProducts",
        "pricing:ListPriceLists",
        "proton:GetDeployment",
        "proton:GetEnvironment",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:ListDeployments",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplates",
        "proton:ListServiceInstances",
        "proton:ListServices",
        "proton:ListServiceTemplates",
        "proton:ListTagsForResource",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ViewPurchaseOrders",
        "qbusiness:GetApplication",
        "qbusiness:GetChatControlsConfiguration",
        "qbusiness:GetDataSource",
        "qbusiness:GetGroup",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetRetriever",
        "qbusiness:GetUser",
        "qbusiness:GetWebExperience",
        "qbusiness:ListApplications",
        "qbusiness:ListDataSources",
        "qbusiness:ListDataSourceSyncJobs",
        "qbusiness:ListGroups",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListSubscriptions",
```

```
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "qldb:DescribeJournalKinesisStream",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "qldb:ListTagsForResource",
        "ram:Get*",
        "ram:List*",
        "rbin:GetRule",
        "rbin:ListRules",
        "rbin:ListTagsForResource",
        "rds:Describe*",
        "rds:Download*",
        "rds:List*",
        "redshift-serverless:GetCustomDomainAssociation",
        "redshift-serverless:GetEndpointAccess",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetRecoveryPoint",
        "redshift-serverless:GetResourcePolicy",
        "redshift-serverless:GetScheduledAction",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetTableRestoreStatus",
        "redshift-serverless:GetUsageLimit",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListCustomDomainAssociations",
        "redshift-serverless:ListEndpointAccess",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListRecoveryPoints",
        "redshift-serverless:ListScheduledActions",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTableRestoreStatus",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListUsageLimits",
        "redshift-serverless:ListWorkgroups",
        "redshift:Describe*",
        "redshift:GetReservedNodeExchangeOfferings",
```

```
        "redshift:ListRecommendations",
        "redshift:View*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetResourcePolicy",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListEnvironmentVpcs",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:CompareFaces",
        "rekognition:DescribeDataset",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DescribeStreamProcessor",
        "rekognition:Detect*",
        "rekognition:GetCelebrityInfo",
        "rekognition:GetCelebrityRecognition",
        "rekognition:GetContentModeration",
        "rekognition:GetFaceDetection",
        "rekognition:GetFaceSearch",
        "rekognition:GetLabelDetection",
        "rekognition:GetPersonTracking",
        "rekognition:GetSegmentDetection",
        "rekognition:GetTextDetection",
        "rekognition:List*",
        "rekognition:RecognizeCelebrities",
        "rekognition:Search*",
        "resiliencehub:GetFailureModeFinding",
        "resiliencehub:GetPolicy",
        "resiliencehub:GetService",
        "resiliencehub:GetSystem",
        "resiliencehub:GetUserJourney",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppAssessment",
        "resiliencehub:DescribeAppVersion",
        "resiliencehub:DescribeAppVersionAppComponent",
        "resiliencehub:DescribeAppVersionResource",
        "resiliencehub:DescribeAppVersionResourcesResolutionStatus",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeDraftAppVersionResourcesImportStatus",
```

```
        "resiliencehub:DescribeMetricsExport",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:DescribeResourceGroupingRecommendationTask",
        "resiliencehub:ListAlarmRecommendations",
        "resiliencehub:ListAppAssessmentComplianceDrifts",
        "resiliencehub:ListAppAssessmentResourceDrifts",
        "resiliencehub:ListAppAssessments",
        "resiliencehub:ListAppComponentCompliances",
        "resiliencehub:ListAppComponentRecommendations",
        "resiliencehub:ListAppInputSources",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionAppComponents",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListAppVersionResources",
        "resiliencehub:ListAppVersions",
        "resiliencehub:ListAssertions",
        "resiliencehub:ListDependencies",
        "resiliencehub:ListFailureModeAssessments",
        "resiliencehub:ListFailureModeFindings",
        "resiliencehub:ListInputSources",
        "resiliencehub:ListMetrics",
        "resiliencehub:ListPolicies",
        "resiliencehub:ListRecommendationTemplates",
        "resiliencehub:ListReports",
        "resiliencehub:ListResources",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListResourceGroupingRecommendations",
        "resiliencehub:ListServices",
        "resiliencehub:ListServiceEvents",
        "resiliencehub:ListServiceFunctions",
        "resiliencehub:ListServiceEvents",
        "resiliencehub:ListServiceFunctions",
        "resiliencehub:ListServiceTopologyEdges",
        "resiliencehub:ListSopRecommendations",
        "resiliencehub:ListSuggestedResiliencyPolicies",
        "resiliencehub:ListSystems",
        "resiliencehub:ListSystemEvents",
        "resiliencehub:ListTagsForResource",
        "resiliencehub:ListTestRecommendations",
        "resiliencehub:ListUnsupportedAppVersionResources",
        "resiliencehub:ListUserJourneys",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:GetAccountLevelServiceConfiguration",
        "resource-explorer-2:GetDefaultView",
```

```
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetManagedView",
        "resource-explorer-2:GetResourceExplorerSetup",
        "resource-explorer-2:GetServiceIndex",
        "resource-explorer-2:GetServiceView",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListIndexesForMembers",
        "resource-explorer-2:ListManagedViews",
        "resource-explorer-2:ListServiceIndexes",
        "resource-explorer-2:ListServiceViews",
        "resource-explorer-2:ListStreamingAccessForServices",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*",
        "robomaker:List*",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-cluster:Get*",
        "route53-recovery-cluster:ListRoutingControls",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53:Test*",
        "route53domains:Check*",
        "route53domains:Get*",
```

```
        "route53domains:List*",
        "route53domains:View*",
        "route53globalresolver:GetAccessSource",
        "route53globalresolver:GetDNSView",
        "route53globalresolver:GetFirewallDomainList",
        "route53globalresolver:GetFirewallRule",
        "route53globalresolver:GetGlobalResolver",
        "route53globalresolver:GetHostedZoneAssociation",
        "route53globalresolver:GetManagedFirewallDomainList",
        "route53globalresolver:ListAccessSources",
        "route53globalresolver:ListAccessTokens",
        "route53globalresolver:ListDNSViews",
        "route53globalresolver:ListFirewallDomainLists",
        "route53globalresolver:ListFirewallDomains",
        "route53globalresolver:ListFirewallRules",
        "route53globalresolver:ListGlobalResolvers",
        "route53globalresolver:ListHostedZoneAssociations",
        "route53globalresolver:ListManagedFirewallDomainLists",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:Get*",
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "s3-object-lambda:GetObject",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectLegalHold",
        "s3-object-lambda:GetObjectRetention",
        "s3-object-lambda:GetObjectTagging",
        "s3-object-lambda:GetObjectVersion",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3-object-lambda:GetObjectVersionTagging",
        "s3-object-lambda:ListBucket",
        "s3-object-lambda:ListBucketMultipartUploads",
        "s3-object-lambda:ListBucketVersions",
        "s3-object-lambda:ListMultipartUploadParts",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
```

```
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetBucketVersioning",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:GetObject",
        "s3-outposts:GetObjectTagging",
        "s3-outposts:GetObjectVersion",
        "s3-outposts:GetObjectVersionForReplication",
        "s3-outposts:GetObjectVersionTagging",
        "s3-outposts:GetReplicationConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListBucket",
        "s3-outposts:ListBucketMultipartUploads",
        "s3-outposts:ListBucketVersions",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListMultipartUploadParts",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListRegionalBuckets",
        "s3-outposts:ListSharedEndpoints",
        "s3:DescribeJob",
        "s3:Get*",
        "s3:List*",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListTagsForResource",
        "s3files:GetAccessPoint",
        "s3files:GetFileSystem",
        "s3files:GetFileSystemPolicy",
        "s3files:GetMountTarget",
        "s3files:GetSynchronizationConfiguration",
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems",
        "s3files:ListMountTargets",
        "s3files:ListTagsForResource",
        "s3tables:GetNamespace",
        "s3tables:GetTable",
        "s3tables:GetTableBucket",
```

```
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:GetTableData",
        "s3tables:GetTableEncryption",
        "s3tables:GetTableMaintenanceConfiguration",
        "s3tables:GetTableMaintenanceJobStatus",
        "s3tables:GetTableMetadataLocation",
        "s3tables:GetTablePolicy",
        "s3tables:GetTableRecordExpirationConfiguration",
        "s3tables:GetTableRecordExpirationJobStatus",
        "s3tables:GetTableReplication",
        "s3tables:GetTableReplicationStatus",
        "s3tables:GetTableStorageClass",
        "s3tables:ListNamespaces",
        "s3tables:ListTableBuckets",
        "s3tables:ListTables",
        "s3tables:ListTagsForResource",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:GetVectors",
        "s3vectors:ListIndexes",
        "s3vectors:ListVectorBuckets",
        "s3vectors:ListVectors",
        "s3vectors:QueryVectors",
        "sagemaker:Describe*",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:List*",
        "sagemaker:Search",
        "savingsplans:DescribeSavingsPlanRates",
        "savingsplans:DescribeSavingsPlans",
        "savingsplans:DescribeSavingsPlansOfferingRates",
        "savingsplans:DescribeSavingsPlansOfferings",
        "savingsplans:ListTagsForResource",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:Describe*",
        "schemas:Get*",
```

```
        "schemas:List*",
        "schemas:Search*",
        "sdb:Get*",
        "sdb:List*",
        "sdb:Select*",
        "secretsmanager:Describe*",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "securityagent:BatchGetAgentSpaces",
        "securityagent:BatchGetArtifactMetadata",
        "securityagent:BatchGetCodeReviewJobs",
        "securityagent:BatchGetCodeReviewJobTasks",
        "securityagent:BatchGetCodeReviews",
        "securityagent:BatchGetFindings",
        "securityagent:BatchGetPentestJobContentMetadata",
        "securityagent:BatchGetPentestJobs",
        "securityagent:BatchGetPentestJobTasks",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetTargetDomains",
        "securityagent:GetApplication",
        "securityagent:GetArtifact",
        "securityagent:GetDesignReview",
        "securityagent:GetDesignReviewArtifact",
        "securityagent:GetDesignReviewFeedback",
        "securityagent:GetIntegration",
        "securityagent:ListAgentSpaces",
        "securityagent:ListApplications",
        "securityagent:ListArtifacts",
        "securityagent:ListCodeReviewJobsForCodeReview",
        "securityagent:ListCodeReviewJobTasks",
        "securityagent:ListCodeReviews",
        "securityagent:ListDesignReviewComments",
        "securityagent:ListDesignReviews",
        "securityagent:ListDiscoveredEndpoints",
        "securityagent:ListSecurityRequirements",
        "securityagent:ListTargetDomains",
        "securityagent:ListFindings",
        "securityagent:ListIntegratedResources",
        "securityagent:ListIntegrations",
        "securityagent:ListMemberships",
        "securityagent:ListPentestJobsForPentest",
        "securityagent:ListPentests",
        "securityagent:ListResourcesFromIntegration",
        "securityagent:ListPentestJobTasks",
```

```
        "securityagent:BatchGetValidationRuns",
        "securityagent:GetSecurityRequirementPack",
        "securityagent:ListDiscoveredDomains",
        "securityagent:ListSecurityRequirementPacks",
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetConfigurationPolicyAssociations",
        "securityhub:BatchGetControlEvaluations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "securitylake:GetDataLakeExceptionSubscription",
        "securitylake:GetDataLakeOrganizationConfiguration",
        "securitylake:GetDataLakeSources",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "serverlessrepo:Get*",
        "serverlessrepo:List*",
        "serverlessrepo:SearchApplications",
        "servicecatalog:Describe*",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:List*",
        "servicecatalog:Scan*",
        "servicecatalog:Search*",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAutoManagementConfiguration",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetQuotaUtilizationReport",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
```

```
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "servicequotas:StartQuotaUtilizationReport",
        "ses:BatchGetMetricData",
        "ses:Describe*",
        "ses:Get*",
        "ses:List*",
        "shield:Describe*",
        "shield:Get*",
        "shield:List*",
        "signer:DescribeSigningJob",
        "signer:GetSigningPlatform",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningJobs",
        "signer:ListSigningPlatforms",
        "signer:ListSigningProfiles",
        "signer:ListTagsForResource",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeAccountLimits",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeProtectConfigurations",
        "sms-voice:DescribeRegistrationAttachments",
        "sms-voice:DescribeRegistrationFieldDefinitions",
        "sms-voice:DescribeRegistrationFieldValues",
        "sms-voice:DescribeRegistrations",
        "sms-voice:DescribeRegistrationSectionDefinitions",
        "sms-voice:DescribeRegistrationTypeDefinitions",
        "sms-voice:DescribeRegistrationVersions",
        "sms-voice:DescribeSenderIds",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "snowball:Describe*",
        "snowball:Get*",
        "snowball:List*",
```

```
        "sns:Check*",
        "sns:Get*",
        "sns:List*",
        "sqs:Get*",
        "sqs:List*",
        "sqs:Receive*",
        "ssm-contacts:DescribeEngagement",
        "ssm-contacts:DescribePage",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListEngagements",
        "ssm-contacts:ListPageReceipts",
        "ssm-contacts:ListPagesByContact",
        "ssm-contacts:ListPagesByEngagement",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResourcePolicies",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-incidents:ListTimelineEvents",
        "ssm-quicksetup:GetConfiguration",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:GetServiceSettings",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-quicksetup:ListConfigurations",
        "ssm-quicksetup:ListQuickSetupTypes",
        "ssm-quicksetup:ListTagsForResource",
        "ssm-sap:GetApplication",
        "ssm-sap:GetComponent",
        "ssm-sap:GetConfigurationCheckOperation",
        "ssm-sap:GetDatabase",
        "ssm-sap:GetOperation",
        "ssm-sap:GetResourcePermission",
        "ssm-sap:ListApplications",
        "ssm-sap:ListComponents",
        "ssm-sap:ListConfigurationCheckDefinitions",
        "ssm-sap:ListConfigurationCheckOperations",
```

```
        "ssm-sap:ListDatabases",
        "ssm-sap:ListOperationEvents",
        "ssm-sap:ListOperations",
        "ssm-sap:ListSubCheckResults",
        "ssm-sap:ListSubCheckRuleResults",
        "ssm-sap:ListTagsForResource",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Search*",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "states:Describe*",
        "states:GetExecutionHistory",
        "states:List*",
        "states:ValidateStateMachineDefinition",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
        "sts:GetCallerIdentity",
        "sts:GetSessionToken",
        "support:DescribeAttachment",
        "support:DescribeCaseAttributes",
        "support:DescribeCases",
        "support:DescribeCommunication",
        "support:DescribeCommunications",
        "support:DescribeCreateCaseOptions",
        "support:DescribeIssueTypes",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeSupportedLanguages",
        "support:DescribeSupportLevel",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "support:SearchForCases",
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
        "sustainability:GetCarbonFootprintSummary",
```

```
        "sustainability:GetEstimatedCarbonEmissions",
        "sustainability:GetEstimatedCarbonEmissionsDimensionValues",
        "sustainability:GetEstimatedWaterAllocation",
        "sustainability:GetEstimatedWaterAllocationDimensionValues",
        "swf:Count*",
        "swf:Describe*",
        "swf:Get*",
        "swf:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "tag:DescribeReportCreation",
        "tag:Get*",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "timestream:DescribeBatchLoadTask",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListBatchLoadTasks",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "tnb:GetSolFunctionInstance",
        "tnb:GetSolFunctionPackage",
        "tnb:GetSolFunctionPackageContent",
        "tnb:GetSolFunctionPackageDescriptor",
        "tnb:GetSolNetworkInstance",
        "tnb:GetSolNetworkOperation",
        "tnb:GetSolNetworkPackage",
        "tnb:GetSolNetworkPackageContent",
        "tnb:GetSolNetworkPackageDescriptor",
        "tnb:ListSolFunctionInstances",
        "tnb:ListSolFunctionPackages",
        "tnb:ListSolNetworkInstances",
        "tnb:ListSolNetworkOperations",
        "tnb:ListSolNetworkPackages",
        "tnb:ListTagsForResource",
        "transcribe:Get*",
```

```
        "transcribe:List*",
        "transfer:Describe*",
        "transfer:List*",
        "transfer:TestIdentityProvider",
        "transform:GetAccountSettings",
        "transform:GetAgent",
        "transform:GetAgentRuntimeConfiguration",
        "transform:GetConnector",
        "transform:ListAgents",
        "transform:ListConnectors",
        "transform:ListProfiles",
        "transform:ListTagsForResource",
        "transform-custom:GetAnalysis",
        "transform-custom:GetCampaign",
        "transform-custom:GetFinding",
        "transform-custom:GetFindingGroups",
        "transform-custom:GetKnowledgeItem",
        "transform-custom:GetRemediation",
        "transform-custom:GetRepository",
        "transform-custom:GetSource",
        "transform-custom:ListAnalyses",
        "transform-custom:ListCampaigns",
        "transform-custom:ListCampaignRepositories",
        "transform-custom:ListFindings",
        "transform-custom:ListKnowledgeItems",
        "transform-custom:ListRemediations",
        "transform-custom:ListRepositories",
        "transform-custom:ListSources",
        "transform-custom:ListTagsForResource",
        "transform-custom:ListTransformationPackageMetadata",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:GetTerminology",
        "translate:ListParallelData",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "trustedadvisor:Describe*",
        "trustedadvisor:GetOrganizationRecommendation",
        "trustedadvisor:GetRecommendation",
        "trustedadvisor:ListChecks",
        "trustedadvisor:ListOrganizationRecommendationAccounts",
        "trustedadvisor:ListOrganizationRecommendationResources",
        "trustedadvisor:ListOrganizationRecommendations",
        "trustedadvisor:ListRecommendationResources",
```

```
        "trustedadvisor:ListRecommendations",
        "user-subscriptions:ListApplicationClaims",
        "user-subscriptions:ListClaims",
        "user-subscriptions:ListUserSubscriptions",
        "uxc:GetAccountColor",
        "uxc:GetAccountCustomizations",
        "uxc:ListServices",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:IsAuthorized",
        "verifiedpermissions:IsAuthorizedWithToken",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetDomainVerification",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListDomainVerifications",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceEndpointAssociations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServiceNetworkVpcEndpointAssociations",
```

```
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:Get*",
        "waf-regional:List*",
        "waf:Get*",
        "waf:List*",
        "wafv2:CheckCapacity",
        "wafv2:Describe*",
        "wafv2:Get*",
        "wafv2:List*",
        "wellarchitected:ExportLens",
        "wellarchitected:GetAnswer",
        "wellarchitected:GetConsolidatedReport",
        "wellarchitected:GetLens",
        "wellarchitected:GetLensReview",
        "wellarchitected:GetLensReviewReport",
        "wellarchitected:GetLensVersionDifference",
        "wellarchitected:GetMilestone",
        "wellarchitected:GetProfile",
        "wellarchitected:GetProfileTemplate",
        "wellarchitected:GetReviewTemplate",
        "wellarchitected:GetReviewTemplateAnswer",
        "wellarchitected:GetReviewTemplateLensReview",
        "wellarchitected:GetWorkload",
        "wellarchitected:List*",
        "workdocs:CheckAlias",
        "workdocs:Describe*",
        "workdocs:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
```

```
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:Describe*",
        "xray:BatchGet*",
        "xray:CancelTraceRetrieval",
        "xray:Get*",
        "xray:ListResourcePolicies",
        "xray:ListRetrievedTraces",
        "xray:ListTagsForResource",
        "xray:StartTraceRetrieval"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ExpressReadOnlySessionObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3express:SessionMode" : "ReadOnly"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ReInventTicketApprovalAccess

Descrição: concede a um usuário ou função do IAM acesso total para visualizar os detalhes da cobrança do passe re:Invent e aprovar o faturamento de suas contas AWS

`ReInventTicketApprovalAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ReInventTicketApprovalAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 10 de junho de 2026, 18:57 UTC
- Horário editado: 10 de junho de 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/ReInventTicketApprovalAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowBillToAWSActions",
      "Effect" : "Allow",
      "Action" : [
        "eventsbilltoaws:info",
        "eventsbilltoaws:approve"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ResourceGroupsandTagEditorFullAccess

Descrição: fornece acesso total ao Resource Groups and ao Tag Editor.

`ResourceGroupsandTagEditorFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ResourceGroupsandTagEditorFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:39 UTC
- Hora da edição: 10 de agosto de 2023, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources",
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ResourceGroupsandTagEditorReadOnlyAccess

Descrição: fornece acesso ao uso do Resource Groups e do Tag Editor, mas não permite a edição de tags via Tag Editor.

`ResourceGroupsandTagEditorReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ResourceGroupsandTagEditorReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:39 UTC
- Hora da edição: 10 de agosto de 2023, 13:42 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ResourceGroupsServiceRolePolicy

Descrição: permite que grupos de AWS recursos consultem os AWS serviços que possuem seus recursos para manter o grupo atualizado

`ResourceGroupsServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 05 de janeiro de 2023, 16:57 UTC
- Hora da edição: 05 de janeiro de 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ResourceGroupsTaggingAPITagUntagSupportedResources

Descrição: fornece permissões para marcar e desmarcar todos os recursos compatíveis com a API Resource Groups Tagging. Essa política também concede as permissões necessárias para recuperar todos os recursos marcados ou previamente marcados por meio da API Resource Groups Tagging.

`ResourceGroupsTaggingAPITagUntagSupportedResources` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ResourceGroupsTaggingAPITagUntagSupportedResources` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário da criação: 11 de outubro de 2024, 11:11 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsTaggingAPITagUntagSupportedResources`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:TagResource",
        "a4b:UntagResource",
        "access-analyzer:TagResource",
        "access-analyzer:UntagResource",
        "acm-pca:TagCertificateAuthority",
        "acm-pca:UntagCertificateAuthority",
        "acm:AddTagsToCertificate",
        "acm:RemoveTagsFromCertificate",
        "amplify:TagResource",
        "amplify:UntagResource",
        "appconfig:TagResource",
        "appconfig:UntagResource",
        "appflow:TagResource",
        "appflow:UntagResource",
        "appmesh:TagResource",
        "appmesh:UntagResource",
```

```
        "appstream:TagResource",
        "appstream:UntagResource",
        "appsync:TagResource",
        "appsync:UntagResource",
        "athena:TagResource",
        "athena:UntagResource",
        "auditmanager:TagResource",
        "auditmanager:UntagResource",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteTags",
        "backup:TagResource",
        "backup:UntagResource",
        "batch:TagResource",
        "batch:UntagResource",
        "braket:TagResource",
        "braket:UntagResource",
        "cassandra:TagResource",
        "cassandra:UntagResource",
        "chime:TagResource",
        "chime:UntagResource",
        "cloud9:TagResource",
        "cloud9:UntagResource",
        "clouddirectory:TagResource",
        "clouddirectory:UntagResource",
        "cloudfront:TagResource",
        "cloudfront:UntagResource",
        "cloudhsm:TagResource",
        "cloudhsm:UntagResource",
        "cloudtrail:AddTags",
        "cloudtrail:RemoveTags",
        "cloudwatch:TagResource",
        "cloudwatch:UntagResource",
        "codeartifact:TagResource",
        "codeartifact:UntagResource",
        "codecommit:TagResource",
        "codecommit:UntagResource",
        "codedeploy:AddTagsToOnPremisesInstances",
        "codedeploy:RemoveTagsFromOnPremisesInstances",
        "codedeploy:TagResource",
        "codedeploy:UntagResource",
        "codeguru-profiler:TagResource",
        "codeguru-profiler:UntagResource",
        "codepipeline:TagResource",
        "codepipeline:UntagResource",
```

```
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar:TagProject",
        "codestar:UntagProject",
        "cognito-identity:TagResource",
        "cognito-identity:UntagResource",
        "cognito-idp:TagResource",
        "cognito-idp:UntagResource",
        "comprehend:TagResource",
        "comprehend:UntagResource",
        "config:TagResource",
        "config:UntagResource",
        "connect:TagResource",
        "connect:UntagResource",
        "dataexchange:TagResource",
        "dataexchange:UntagResource",
        "datapipeline:AddTags",
        "datapipeline:RemoveTags",
        "datasync:TagResource",
        "datasync:UntagResource",
        "deepcomposer:TagResource",
        "deepcomposer:UntagResource",
        "detective:TagResource",
        "detective:UntagResource",
        "devicefarm:TagResource",
        "devicefarm:UntagResource",
        "directconnect:TagResource",
        "directconnect:UntagResource",
        "dlm:TagResource",
        "dlm:UntagResource",
        "dms:AddTagsToResource",
        "dms:RemoveTagsFromResource",
        "dynamodb:TagResource",
        "dynamodb:UntagResource",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ecr:TagResource",
        "ecr:UntagResource",
        "ecs:TagResource",
        "ecs:UntagResource",
        "eks:TagResource",
        "eks:UntagResource",
        "elastic-inference:TagResource",
        "elastic-inference:UntagResource",
```

```
        "elasticache:AddTagsToResource",
        "elasticache:RemoveTagsFromResource",
        "elasticbeanstalk:UpdateTagsForResource",
        "elasticfilesystem:CreateTags",
        "elasticfilesystem:DeleteTags",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:RemoveTags",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
        "emr-containers:TagResource",
        "emr-containers:UntagResource",
        "es:AddTags",
        "es:RemoveTags",
        "events:TagResource",
        "events:UntagResource",
        "firehose:TagDeliveryStream",
        "firehose:UntagDeliveryStream",
        "fms:TagResource",
        "fms:UntagResource",
        "forecast:TagResource",
        "forecast:UntagResource",
        "frauddetector:TagResource",
        "frauddetector:UntagResource",
        "fsx:TagResource",
        "fsx:UntagResource",
        "gamelift:TagResource",
        "gamelift:UntagResource",
        "glacier:AddTagsToVault",
        "glacier:RemoveTagsFromVault",
        "globalaccelerator:TagResource",
        "globalaccelerator:UntagResource",
        "glue:TagResource",
        "glue:UntagResource",
        "greengrass:TagResource",
        "greengrass:UntagResource",
        "groundstation:TagResource",
        "groundstation:UntagResource",
        "guardduty:TagResource",
        "guardduty:UntagResource",
        "iam:TagInstanceProfile",
        "iam:TagMFADevice",
        "iam:TagOpenIDConnectProvider",
        "iam:TagPolicy",
        "iam:TagRole",
```

```
        "iam:TagSAMLProvider",
        "iam:TagServerCertificate",
        "iam:TagUser",
        "iam:UntagInstanceProfile",
        "iam:UntagMFADevice",
        "iam:UntagOpenIDConnectProvider",
        "iam:UntagPolicy",
        "iam:UntagRole",
        "iam:UntagSAMLProvider",
        "iam:UntagServerCertificate",
        "iam:UntagUser",
        "imagebuilder:TagResource",
        "imagebuilder:UntagResource",
        "inspector:ListTagsForResource",
        "inspector:SetTagsForResource",
        "iot1click:TagResource",
        "iot1click:UntagResource",
        "iot:TagResource",
        "iot:UntagResource",
        "iotanalytics:TagResource",
        "iotanalytics:UntagResource",
        "iotdeviceadvisor:TagResource",
        "iotdeviceadvisor:UntagResource",
        "iotevents:TagResource",
        "iotevents:UntagResource",
        "iotfleethub:TagResource",
        "iotfleethub:UntagResource",
        "iotsitewise:TagResource",
        "iotsitewise:UntagResource",
        "iottwinmaker:TagResource",
        "iottwinmaker:UntagResource",
        "iotwireless:TagResource",
        "iotwireless:UntagResource",
        "ivs:TagResource",
        "ivs:UntagResource",
        "kafka:TagResource",
        "kafka:UntagResource",
        "kendra:TagResource",
        "kendra:UntagResource",
        "kinesis:AddTagsToStream",
        "kinesis:RemoveTagsFromStream",
        "kinesisanalytics:TagResource",
        "kinesisanalytics:UntagResource",
        "kms:TagResource",
```

```
        "kms:UntagResource",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lex:TagResource",
        "lex:UntagResource",
        "license-manager:TagResource",
        "license-manager:UntagResource",
        "lightsail:TagResource",
        "lightsail:UntagResource",
        "logs:TagLogGroup",
        "logs:TagResource",
        "logs:UntagLogGroup",
        "logs:UntagResource",
        "lookoutequipment:TagResource",
        "lookoutequipment:UntagResource",
        "machinelearning:AddTags",
        "machinelearning:DeleteTags",
        "macie2:TagResource",
        "macie2:UntagResource",
        "managedblockchain:TagResource",
        "managedblockchain:UntagResource",
        "mediaconnect:TagResource",
        "mediaconnect:UntagResource",
        "mediaconvert:TagResource",
        "mediaconvert:UntagResource",
        "medialive:CreateTags",
        "medialive:DeleteTags",
        "mediapackage-vod:TagResource",
        "mediapackage-vod:UntagResource",
        "mediapackage:TagResource",
        "mediapackage:UntagResource",
        "mediatailor:TagResource",
        "mediatailor:UntagResource",
        "mobiletargeting:TagResource",
        "mobiletargeting:UntagResource",
        "mq:CreateTags",
        "mq:DeleteTags",
        "neptune-graph:TagResource",
        "neptune-graph:UntagResource",
        "network-firewall:TagResource",
        "network-firewall:UntagResource",
        "networkmanager:TagResource",
        "networkmanager:UntagResource",
        "opsworks-cm:TagResource",
```

```
        "opsworks-cm:UntagResource",
        "opsworks:TagResource",
        "opsworks:UntagResource",
        "organizations:TagResource",
        "organizations:UntagResource",
        "outposts:TagResource",
        "outposts:UntagResource",
        "qldb:TagResource",
        "qldb:UntagResource",
        "quicksight:TagResource",
        "quicksight:UntagResource",
        "ram:TagResource",
        "ram:UntagResource",
        "rds:AddTagsToResource",
        "rds:RemoveTagsFromResource",
        "redshift:CreateTags",
        "redshift:DeleteTags",
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
        "resource-groups:Tag",
        "resource-groups:Untag",
        "robomaker:TagResource",
        "robomaker:UntagResource",
        "route53:ChangeTagsForResource",
        "route53domains:DeleteTagsForDomain",
        "route53domains:UpdateTagsForDomain",
        "route53resolver:TagResource",
        "route53resolver:UntagResource",
        "s3:GetBucketTagging",
        "s3:GetJobTagging",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionTagging",
        "s3:GetStorageLensConfigurationTagging",
        "s3:DeleteJobTagging",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging",
        "s3:PutBucketTagging",
        "s3:PutJobTagging",
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging",
        "s3:PutStorageLensConfigurationTagging",
        "s3:DeleteStorageLensConfigurationTagging",
        "s3:TagResource",
        "s3:UntagResource",
```

```
        "sagemaker:AddTags",
        "sagemaker:DeleteTags",
        "savingsplans:TagResource",
        "savingsplans:UntagResource",
        "schemas:TagResource",
        "schemas:UntagResource",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource",
        "securityhub:TagResource",
        "securityhub:UntagResource",
        "servicediscovery:TagResource",
        "servicediscovery:UntagResource",
        "servicequotas:TagResource",
        "servicequotas:UntagResource",
        "ses:TagResource",
        "ses:UntagResource",
        "sns:TagResource",
        "sns:UntagResource",
        "sqs:TagQueue",
        "sqs:UntagQueue",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "states:TagResource",
        "states:UntagResource",
        "storagegateway:AddTagsToResource",
        "storagegateway:RemoveTagsFromResource",
        "swf:TagResource",
        "swf:UntagResource",
        "synthetics:TagResource",
        "synthetics:UntagResource",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "transfer:TagResource",
        "transfer:UntagResource",
        "waf-regional:TagResource",
        "waf-regional:UntagResource",
        "waf:TagResource",
        "waf:UntagResource",
        "wafv2:TagResource",
        "wafv2:UntagResource",
        "worklink:TagResource",
        "worklink:UntagResource",
        "workmail:TagResource",
```

```
        "workmail:UntagResource",
        "workspaces:CreateTags",
        "workspaces:DeleteTags",
        "xray:TagResource",
        "xray:UntagResource",
        "kinesisvideo:TagResource",
        "kinesisvideo:UntagResource",
        "redshift-serverless:TagResource",
        "redshift-serverless:UntagResource",
        "route53-recovery-control-config:TagResource",
        "route53-recovery-control-config:UntagResource",
        "route53-recovery-readiness:TagResource",
        "route53-recovery-readiness:UntagResource",
        "ssm-contacts:TagResource",
        "ssm-contacts:UntagResource",
        "ssm-incidents:TagResource",
        "ssm-incidents:UntagResource",
        "vpc-lattice:TagResource",
        "vpc-lattice:UntagResource",
        "workspaces-web:TagResource",
        "workspaces-web:UntagResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ROSAAmazonEBSCSIDriverOperatorPolicy

Descrição: Permite que o operador do driver OpenShift Amazon EBS Container Storage Interface (CSI) instale e mantenha o driver CSI do Amazon EBS em um cluster Red Hat OpenShift Service on AWS (ROSA). O driver da CSI do Amazon EBS permite que os clusters do ROSA gerenciem o ciclo de vida dos volumes do Amazon EBS para os volumes persistentes.

`ROSAAmazonEBSCSIDriverOperatorPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ROSAAmazonEBSCSIDriverOperatorPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 20 de abril de 2023, 22:36 UTC
- Horário editado: 19 de agosto de 2026, 05:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyDescribeOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateAndCopyVolumesWithManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CopyManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/vol-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CopyUserBroughtVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/vol-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "CreateSnapshotsWithManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsFromManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsFromUserBroughtVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "ManageManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:AttachVolume",
```

```
        "ec2:DetachVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ManageUserBroughtVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateVolumesFromAndEnableFSROnManagedSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateVolumesFromAndEnableFSROnUserBroughtSnapshots",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "AttachDetachVolumesToManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteAndLockManagedSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteAndLockUserBroughtSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "TagResourcesOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot",
            "CopyVolumes"
          ]
        }
      }
    },
    {
      "Sid" : "ModifyTagsOnManagedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringNotEquals" : {
```

```
          "aws:TagKeys" : [
            "red-hat-managed",
            "ebs.csi.aws.com/cluster",
            "kubernetes.io/created-for/pvc/name"
          ]
        }
      }
    },
    {
      "Sid" : "ModifyTagsOnUserBroughtVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringNotEquals" : {
          "aws:TagKeys" : [
            "red-hat-managed",
            "red-hat",
            "ebs.csi.aws.com/cluster",
            "kubernetes.io/created-for/pvc/name"
          ]
        }
      }
    },
    {
      "Sid" : "KMSEncryptedVolumes",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : false
        },
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "StringEquals" : {
          "kms:GrantConstraintType" : "EncryptionContextSubset",
          "aws:ResourceTag/red-hat" : "true"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : false
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo"
          ],
```

```
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeKMSKeysForEBSVolumeEncryption",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ROSACloudNetworkConfigOperatorPolicy

Descrição: Permite que o OpenShift Cloud Network Config Controller Operator provisione e gerencie recursos de rede para uso pela sobreposição de rede de cluster Red Hat OpenShift Service on AWS (ROSA). O OpenShift Cloud Network Operator interage com AWS APIs em nome dos plug-ins de rede via CustomResourceDefinitions. O operador usa essas permissões de política para gerenciar endereços IP privados para instâncias do Amazon EC2 como parte do cluster ROSA.

`ROSACloudNetworkConfigOperatorPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ROSACloudNetworkConfigOperatorPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 20 de abril de 2023, 22:34 UTC
- Hora da edição: 20 de abril de 2023, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModifyEIPs",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ROSAControlPlaneOperatorPolicy

Descrição: permite que o plano de controle do Red Hat OpenShift Service on AWS (ROSA) gerencie os recursos do cluster ROSA Amazon EC2 e Amazon Route 53.

`ROSAControlPlaneOperatorPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ROSAControlPlaneOperatorPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 24 de abril de 2023, 23:02 UTC

- Horário editado: 28 de julho de 2026, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "route53:ListHostedZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
```

```
    {
      "Sid" : "ListResourceRecordSets",
      "Effect" : "Allow",
      "Action" : [
        "route53:ListResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ChangeResourceRecordSetsRestrictedRecordNames",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.hypershift.local"
          ]
        }
      }
    },
    {
      "Sid" : "VPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointResourceTagCondition",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "ManageVPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVPCEndpointNoCondition",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpcEndpoint",
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "AddDeleteTagsRedHatManagedSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        },
        "ForAllValues:StringNotEquals" : {
          "aws:TagKeys" : [
            "red-hat-managed"
```

```
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ROSAImageRegistryOperatorPolicy

Descrição: permite que o operador de registro de OpenShift imagens provisione e gerencie buckets e objetos do Amazon S3 para uso pelo Red Hat OpenShift Service on AWS (ROSA) no registro de imagens no cluster para atender aos requisitos de armazenamento do ROSA. O OpenShift Image Registry Operator instala e mantém o registro interno de um OpenShift cluster Red Hat.

`ROSAImageRegistryOperatorPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ROSAImageRegistryOperatorPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 27 de abril de 2023, 20:13 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSpecificBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}?",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}"
      ]
```

```
    },
    {
      "Sid" : "AllowSpecificObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*/*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}?/*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ROSAIngressOperatorPolicy

Descrição: Permite que o OpenShift Ingress Operator provisione e gerencie balanceadores de carga e configurações de sistema de nomes de domínio (DNS) para clusters Red Hat OpenShift Service on AWS (ROSA). A política permite acesso de leitura aos valores das tags, que o operador filtra para os recursos do Route 53 para descobrir zonas hospedadas.

`ROSAIngressOperatorPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ROSAIngressOperatorPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 20 de abril de 2023, 22:37 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "route53:ListHostedZones",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.openshiftapps.com",
            "*.devshift.org",
```

```
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ROSAInstallerPolicy

Descrição: Permite que o instalador do Red Hat OpenShift Service on AWS (ROSA) gerencie AWS recursos que suportam a instalação do cluster ROSA. Isso inclui o gerenciamento de perfis de instância para nós de trabalho ROSA.

`ROSAInstallerPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ROSAInstallerPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 06 de junho de 2023, 21:00 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeCapacityReservations",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetOpenIDConnectProvider",
        "iam:GetRole",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53:GetAccountLimit",
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToEC2",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ]
    },
    {
      "Sid" : "CreateInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:TagInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "GetSecretValue",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "Route53ManageRecords",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.hypershift.local",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    },
    {
      "Sid" : "Route53Manage",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeTagsForResource",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "RunInstancesNoCondition",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RunInstancesRestrictedRequestTag",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesRedHatOwnedAMIs",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822",
            "210686502322"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstancesRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateGrantRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
```

```
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsK8sSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteTagsK8sSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "ListPoliciesAttachedToRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ROSAKarpenterControllerPolicy

Descrição: Fornece permissões para o controlador ROSA Karpenter provisionar e gerenciar dinamicamente instâncias do EC2 para clusters de planos de controle hospedados pelo Red Hat OpenShift Service on AWS (ROSA). Isso inclui gerenciamento do ciclo de vida de frotas e instâncias do EC2, consultas de preços de instâncias, operações de KMS para criptografia de volume do EBS com chaves gerenciadas pelo cliente e gerenciamento de perfis de instâncias do IAM.

`ROSAKarpenterControllerPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ROSAKarpenterControllerPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 27 de julho de 2026, 16:42 UTC
- Horário editado: 27 de julho de 2026, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKarpenterControllerPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "PricingReadActions",
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeKMSKeysForEBSVolumeEncryption",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CryptoOpsForEBSVolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "CreateGrantForEBSVolumeEncryption",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "StringEquals" : {
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo"
          ],
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ]
    },
    {
      "Sid" : "CreateEC2ResourcesWithApprovedAMIs",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822",
            "210686502322"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEC2ResourcesWithTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEC2ResourcesLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateFleet",
            "CreateLaunchTemplate"
          ],
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ManageTagsOnManagedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "TerminateManagedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "PassInstanceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*-ROSA-Worker-Role",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
```

```
      ]
    },
    {
      "Sid" : "CreateInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:TagInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ReadInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ROSAKMSProviderPolicy

Descrição: permite que o provedor de AWS criptografia ROSA integrado gerencie as chaves do Serviço de Gerenciamento de Chaves (KMS) para oferecer suporte à criptografia de dados etcd usando uma AWS chave AWS KMS fornecida pelo cliente. A política permite a criptografia e a descriptografia de dados usando chaves KMS.

`ROSAKMSProviderPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ROSAKMSProviderPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 27 de abril de 2023, 20:10 UTC
- Hora da edição: 27 de abril de 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
```

```
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ROSAKubeControllerPolicy

Descrição: permite que o controlador ROSA Kubernetes gerencie os recursos do Amazon EC2, do Elastic Load Balancing (ELB) e do AWS Key Management Service (KMS) para um cluster ROSA.

`ROSAKubeControllerPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ROSAKubeControllerPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 27 de abril de 2023, 20:09 UTC
- Horário editado: 17 de setembro de 2026, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy`

Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeLoadBalancerPolicies"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "LoadBalanacerManagement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancerPolicy",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateTargetGroup",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "LoadBalanacerManagementResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteListener",
```

```
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:SetSecurityGroups",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:DeleteLoadBalancerListeners",
        "elasticloadbalancing:AttachLoadBalancerToSubnets",
        "elasticloadbalancing:DetachLoadBalancerFromSubnets",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateListeners",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true",
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateLoadBalancer",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ModifySecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "ManageTargetGroup",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center

- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ROSAManageSubscription

Descrição: Essa política fornece as permissões necessárias para gerenciar a assinatura Red Hat OpenShift Service on AWS (ROSA).

`ROSAManageSubscription` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ROSAManageSubscription` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 11 de abril de 2022, 20:58 UTC
- Hora da edição: 04 de agosto de 2023, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/ROSAManageSubscription`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "34850061-abaf-402d-92df-94325c9e947f",
            "bfdca560-2c78-4e64-8193-794c159e6d30"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ROSANodePoolManagementPolicy

Descrição: permite que o Red Hat OpenShift Service on AWS (ROSA) gerencie instâncias EC2 de cluster como nós de trabalho, incluindo permissão para configurar grupos de segurança e marcar instâncias e volumes. Essa política também permite o uso de instâncias do EC2 com criptografia de disco fornecida pelas AWS chaves do Key Management Service (KMS).

`ROSANodePoolManagementPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ROSANodePoolManagementPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 08 de junho de 2023, 20:48 UTC
- Horário editado: 29 de julho de 2026, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassWorkerRole",
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AuthorizeSecurityGroupIngressRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfacesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileInstance",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesRequest",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesNoCondition",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ]
    },
    {
      "Sid" : "RunInstancesRedHatAMI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822"
          ]
        }
      }
    },
    {
      "Sid" : "NodePoolSQSActions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:DeleteMessage",
        "sqs:ReceiveMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateGrantRestricted",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ROSASharedVPCEndpointPolicy

Descrição: permite que o instalador do Red Hat OpenShift Service on AWS (ROSA) configure VPC Endpoints e Security Groups. Destinada a ser usada em uma VPC compartilhada.

`ROSASharedVPCEndpointPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ROSASharedVPCEndpointPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 11 de agosto de 2025, 17:19 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/ROSASharedVPCEndpointPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "VPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointResourceTagCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "ManageVPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVPCEndpoingNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
```

```
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpcEndpoint",
            "CreateSecurityGroup"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ROSASharedVPCRoute53Policy

Descrição: Permite que o instalador do Red Hat OpenShift Service on AWS (ROSA) configure os registros do Route53. Destinada a ser usada em uma VPC compartilhada.

`ROSASharedVPCRoute53Policy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ROSASharedVPCRoute53Policy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 11 de agosto de 2025, 17:19 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/ROSASharedVPCRoute53Policy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ChangeResourceRecordSetsRestrictedRecordNames",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ],
```

```
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.hypershift.local",
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    },
    {
      "Sid" : "ChangeTagsForResourceNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ROSASRESupportPolicy

Descrição: Fornece à engenharia de confiabilidade de sites (SRE) do ROSA as permissões necessárias para observar, diagnosticar e dar suporte inicialmente aos AWS recursos associados aos clusters Red Hat OpenShift Service on AWS (ROSA), incluindo a capacidade de alterar o estado do nó do cluster ROSA.

`ROSASRESupportPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ROSASRESupportPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 01 de junho de 2023, 14:36 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "sts:DecodeAuthorizationMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHostedZoneCount",
```

```
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DecribeIAMRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2DescribeInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeScheduledInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "VPCNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "Cloudtrail",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Cloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeLoadBalancers",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListenerCertificates",
```

```
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeAddressesAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeAddressesAttribute",
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*"
    },
```

```
    {
      "Sid" : "DescribeInstance",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeSpotFleetInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSpotFleetInstances",
      "Resource" : "arn:aws:ec2:*:*:spot-fleet-request/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeVolumeAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeVolumeAttribute",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ManageInstanceLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ROSAWorkerInstancePolicy

Descrição: Permite que os nós de trabalho do Red Hat OpenShift Service on AWS (ROSA) em sua conta tenham acesso somente para leitura às instâncias do Amazon EC2 e Regiões da AWS para o gerenciamento do ciclo de vida dos nós de computação.

`ROSAWorkerInstancePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ROSAWorkerInstancePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 20 de abril de 2023, 22:35 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2DescribeInstancesRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECRGetAuthorizationToken",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECRReadOnlyAccessRedHatManaged",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:ListTagsForResource"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

Route53RecoveryReadinessServiceRolePolicy

Descrição: política de perfil vinculado ao serviço para preparação para recuperação do Route 53

`Route53RecoveryReadinessServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 15 de julho de 2021, 16:06 UTC
- Hora da edição: 14 de fevereiro de 2023, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicequotas.amazonaws.com/
AWSServiceRoleForServiceQuotas",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:ListAliases",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBClusters"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ListResourceRecordSets"
      ],
      "Resource" : "arn:aws:route53:::hostedzone/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHealthCheck",
        "route53:GetHealthCheckStatus"
      ],
      "Resource" : "arn:aws:route53:::healthcheck/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:RequestServiceQuotaIncrease"
```

```
      ],
      "Resource" : "arn:aws:servicequotas:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ],
      "Resource" : "arn:aws:sqs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeLoadBalancerTargetGroups",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribePolicies",
        "cloudwatch:GetMetricData",
        "cloudwatch:DescribeAlarms",
        "dynamodb:DescribeLimits",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "kafka:DescribeCluster",
        "kafka:DescribeConfigurationRevision",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "rds:DescribeAccountAttributes",
        "route53:GetHostedZone",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "sns:GetEndpointAttributes",
        "sns:GetSubscriptionAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

Route53ResolverServiceRolePolicy

Descrição: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo Route53 Resolver

`Route53ResolverServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 12 de agosto de 2020, 17:47 UTC
- Hora da edição: 12 de agosto de 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "s3:GetBucketPolicy"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

RTBFabricServiceRolePolicy

Descrição: Uma função vinculada ao serviço necessária para que o AWS RTBFabric crie e gerencie seus recursos de interface de rede e forneça métricas.

`RTBFabricServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 16 de outubro de 2025, 16:49 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/RTBFabricServiceRolePolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RTBFabricRoleCreateNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "RTBFabricRoleCreateTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/RTBFabricManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleCreateNetworkInterfacePermissionActions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/RTBFabricManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleModifyTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/RTBFabricManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RTBFabricRolePutMetricDataActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/RTBFabric"
```

```
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

S3StorageLensServiceRolePolicy

Descrição: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo S3 Storage Lens

`S3StorageLensServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 18 de novembro de 2020, 18:15 UTC
- Hora da edição: 18 de novembro de 2020, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioAdminIAMConsolePolicy

Descrição: Fornece privilégios iniciais de configuração administrativa e individual para o Amazon SageMaker Unified Studio por meio do SDK Console de gerenciamento da AWS e. Permite o lançamento do SageMaker Unified Studio Portal.

`SageMakerStudioAdminIAMConsolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioAdminIAMConsolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 18 de agosto de 2025, 22:49 UTC
- Horário editado: 26 de agosto de 2026, 22:47 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMConsolePolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
```

```
        "iam:GetRole",
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*"
      ]
    },
    {
      "Sid" : "DescribeEc2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTaggedEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpc"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSubnetInTaggedVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSubnet"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedSecurityGroupInVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateVPCEndpointInTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateInternetGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway"
      ],
      "Resource" : "arn:aws:ec2:*:*:internet-gateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedNatGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:natgateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNatGatewayInTaggedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRouteTableInTaggedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRouteTable"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AllocateAddress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyTaggedEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcAttribute",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AttachInternetGateway",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:AttachInternetGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRoute",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AssociateRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "Ec2TaggingOperations",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true",
          "ec2:CreateAction" : [
            "CreateVpc",
            "CreateSubnet",
            "CreateSecurityGroup",
            "CreateInternetGateway",
            "CreateNatGateway",
            "CreateRouteTable",
            "CreateVpcEndpoint"
          ]
        }
      }
    },
    {
      "Sid" : "Ec2TagEIP",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AllowCFNStackCreation",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:CreateStack",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateStack"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteTaggedVpcResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpc",
        "ec2:DeleteSubnet",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteInternetGateway",
        "ec2:DetachInternetGateway",
        "ec2:DeleteNatGateway",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteRouteTable",
        "ec2:DeleteRoute",
        "ec2:ReleaseAddress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteTagsOnTaggedResources",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteTags",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "S3ReadCFNTemplate",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "DataZoneKMSGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueCatalogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOApplicationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DeleteApplication"
      ],
      "Resource" : [
        "arn:aws:sso::*:application/*/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSOKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioAdminIAMDefaultExecutionPolicy

Descrição: Política de execução administrativa para usar funções do IAM com o SageMaker Unified Studio. Permite que os administradores provisionem, gerenciem e acessem recursos em sua conta (excluindo o acesso aos recursos de dados) para IAM-based uso do SageMaker Unified Studio.

`SageMakerStudioAdminIAMDefaultExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioAdminIAMDefaultExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 18 de agosto de 2025, 17:19 UTC
- Horário editado: 14 de julho de 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMDefaultExecutionPolicy`

Versão da política

Versão da política: v24 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SageMakerUnifiedStudioMcp",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker-unified-studio-mcp:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:GetUser",
        "iam:ListUsers",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless",
        "arn:aws:iam::*:role/aws-service-role/ops.athena.amazonaws.com/
AWSServiceRoleForAmazonAthena"
      ]
    },
    {
```

```
      "Sid" : "TagRoleAndSession",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "sts:TagSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "SageMakerSpacesDomainId"
          ]
        }
      }
    },
    {
      "Sid" : "CreateRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ]
    },
    {
      "Sid" : "AttachPolicy",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy",
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
```

```
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "PassRoleForProvisioning",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "athena.amazonaws.com",
            "glue.amazonaws.com",
            "datazone.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
        "arn:aws:iam::*:role/${aws:PrincipalTag/AmazonDataZonePassedRolePath}"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "datazone.amazonaws.com",
            "bedrock.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
```

```
            "redshift.amazonaws.com",
            "airflow-serverless.amazonaws.com",
            "events.amazonaws.com",
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "Q",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "q:Get*",
        "q:List*",
        "q:PassRequest",
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:GetParameter*",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "ManageSageMakerSpace",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*"
```

```
      ]
    },
    {
      "Sid" : "ResourceGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:Batch*",
        "sagemaker:DeleteTags",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sagemaker:Search",
        "sagemaker:*Endpoint*",
        "sagemaker:*Model*",
        "sagemaker:*Context*",
        "sagemaker:*Artifact*",
        "sagemaker:*Action*",
        "sagemaker:*Association*",
        "sagemaker:QueryLineage",
        "sagemaker:*InferenceComponent*",
        "sagemaker:*Job*",
        "sagemaker:*MlflowApp*",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*",
        "sagemaker:*Feature*",
        "sagemaker:*Record"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateBucket",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:CreateBucket",
        "s3:DeleteBucketPolicy",
        "s3:Get*",
        "s3:Put*",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "S3List",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:List*",
        "s3:PutObject*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*",
        "arn:aws:cloudformation:*:*:transform/*"
```

```
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "LogsAndMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:GetMetricData",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:Describe*",
        "logs:Get*",
        "logs:PutLogEvents",
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LFManage",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DeregisterResource",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:CreateLakeFormationOptIn",
```

```
        "lakeformation:DeleteLakeFormationOptIn",
        "lakeformation:*DataCellsFilter"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:connection/*"
      ]
    },
    {
      "Sid" : "GlueLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "Glue",
      "Effect" : "Allow",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:Describe*",
        "glue:Get*",
        "glue:List*",
        "glue:NotifyEvent",
        "glue:RunStatement",
```

```
        "glue:StartCompletion",
        "glue:StopSession",
        "glue:*Resource",
        "glue:UseGlueStudio",
        "glue:*Job*",
        "glue:TestConnection",
        "glue:*DataQuality*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyForeignSessionAccess",
      "Effect" : "Deny",
      "Action" : [
        "athena:GetResourceDashboard",
        "athena:GetSession",
        "athena:GetSessionEndpoint",
        "athena:GetSessionStatus",
        "athena:StartSession",
        "athena:TerminateSession",
        "emr-serverless:*Session*",
        "emr-serverless:*Dashboard*",
        "emr-containers:*ManagedEndpoint*",
        "elasticmapreduce:*Session*",
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetDashboardUrl",
        "glue:GetSession",
        "glue:GetSessionEndpoint",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
```

```
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource",
        "emr-serverless:*Resource",
        "emr-containers:*Resource",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "SQLWorkBench",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftData",
      "Effect" : "Allow",
      "Action" : "redshift-data:*",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedShiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:Describe*",
        "redshift-data:ExecuteStatement",
        "redshift-data:List*",
        "redshift-serverless:GetManagedWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Bedrock",
      "Effect" : "Allow",
      "Action" : "bedrock:*",
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Athena",
```

```
      "Effect" : "Allow",
      "Action" : [
        "athena:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowServerless",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:List*",
        "airflow-serverless:Get*",
        "airflow-serverless:CreateWorkflow",
        "airflow-serverless:UpdateWorkflow",
        "airflow-serverless:DeleteWorkflow",
        "airflow-serverless:StartWorkflowRun",
        "airflow-serverless:StopWorkflowRun",
        "airflow-serverless:TagResource",
        "airflow-serverless:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowMWAA",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManagePrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy",
```

```
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*"
    },
```

```
    {
      "Sid" : "GenerateRecommendations",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageScheduler",
      "Effect" : "Allow",
      "Action" : "scheduler:*",
      "Resource" : "*"
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsAdmin",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:*",
        "codestar-connections:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
```

```
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
```

```
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
```

```
    {
      "Sid" : "SGManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "SGCreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
```

```
            "AmazonDataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "aws:cloudformation:*"
          ]
        }
      }
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "EMR",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:Get*",
        "emr-serverless:List*",
        "emr-serverless:Start*",
        "emr-serverless:Access*",
        "emr-serverless:Terminate*",
        "emr-serverless:*Resource",
        "emr-containers:*ManagedEndpoint*",
        "emr-containers:*SecurityConfiguration*",
        "emr-containers:*VirtualCluster*",
        "emr-containers:*Resource",
```

```
        "elasticmapreduce:*PersistentAppUI*",
        "elasticmapreduce:Start*",
        "elasticmapreduce:Get*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elasticmapreduce:Terminate*",
        "elasticmapreduce:*Tag*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOApplicationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationAccessScope",
        "sso:UpdateApplication",
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplicationAssignment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "SSOReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IdentityStoreKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "RAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:Get*",
        "ram:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMCreateResourcePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RAMResourceSharePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RAMAssociateResourceSharePermission",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    },
    {
      "Sid" : "CanvasGeneralPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "comprehend:*",
        "textract:*",
        "rekognition:*",
        "sagemaker-data-science-assistant:*",
        "rds:DescribeDBInstances",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalingActivities",
        "quicksight:ListNamespaces",
        "events:PutRule",
        "events:DescribeRule",
        "events:PutTargets",
        "events:TagResource",
        "events:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CanvasRedshiftAccess",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioAdminIAMPermissiveExecutionPolicy

Descrição: Política de execução administrativa para usar funções do IAM com o SageMaker Unified Studio. Permite que os administradores provisionem, gerenciem e acessem recursos na conta local (incluindo amplo acesso a todas as APIs em serviços de dados como S3, Glue, CloudWatch Logs e outros) para IAM-based uso do Unified Studio. SageMaker

`SageMakerStudioAdminIAMPermissiveExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioAdminIAMPermissiveExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 18 de agosto de 2025, 17:19 UTC
- Horário editado: 14 de julho de 2026, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMPermissiveExecutionPolicy`

Versão da política

Versão da política: v21 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:*",
        "glue:*",
        "logs:*",
        "redshift-data:*",
        "redshift-serverless:*",
        "redshift:*",
        "s3:*",
        "s3tables:*",
        "comprehend:*",
        "textract:*",
        "rekognition:*",
        "sagemaker-data-science-assistant:*",
        "rds:*",
        "quicksight:*",
        "events:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeAccess",
      "Effect" : "Allow",
      "Action" : [
        "athena:*",
        "bedrock:*",
        "codewhisperer:*",
        "sagemaker-unified-studio-mcp:*",
        "datazone:*",
        "elasticmapreduce:*",
        "emr-containers:*",
        "q:*",
        "sagemaker:*",
        "sagemaker-mlflow:*",
        "scheduler:*",
        "sqlworkbench:*",
        "emr-serverless:*",
        "airflow-serverless:*",
        "airflow:*",
        "application-autoscaling:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CfnManage",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*",
        "arn:aws:cloudformation:*:*:transform/*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "DenyForeignSessionAccess",
      "Effect" : "Deny",
      "Action" : [
        "athena:GetResourceDashboard",
        "athena:GetSession",
        "athena:GetSessionEndpoint",
        "athena:GetSessionStatus",
        "athena:StartSession",
        "athena:TerminateSession",
        "emr-serverless:*Session*",
        "emr-serverless:*Dashboard*",
        "emr-containers:*ManagedEndpoint*",
        "elasticmapreduce:*Session*",
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetDashboardUrl",
        "glue:GetSession",
        "glue:GetSessionEndpoint",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
```

```
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource",
        "emr-serverless:*Resource",
        "emr-containers:*Resource",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:GetUser",
        "iam:ListUsers",
        "sts:AssumeRole"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless",
        "arn:aws:iam::*:role/aws-service-role/ops.athena.amazonaws.com/
AWSServiceRoleForAmazonAthena"
      ]
    },
    {
      "Sid" : "TagRoleAndSession",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "sts:TagSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "SageMakerSpacesDomainId"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "PassRoleForProvisioning",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "athena.amazonaws.com",
            "glue.amazonaws.com",
            "datazone.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
        "arn:aws:iam::*:role/${aws:PrincipalTag/AmazonDataZonePassedRolePath}"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com",
            "datazone.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "airflow-serverless.amazonaws.com",
            "pods.eks.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "CreateRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ]
    },
    {
      "Sid" : "AttachPolicy",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy",
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
```

```
        "ssm:GetParameter*",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DeregisterResource",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteLakeFormationOptIn",
        "lakeformation:*DataCellsFilter"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets",
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManagePrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*"
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnections",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:*",
        "codestar-connections:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
```

```
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
```

```
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
```

```
    {
      "Sid" : "SGManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "SGCreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
```

```
            "AmazonDataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "aws:cloudformation:*"
          ]
        }
      }
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "SSOApplicationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationAccessScope",
        "sso:UpdateApplication",
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplicationAssignment"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "SSOReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IdentityStoreKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "RAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:Get*",
        "ram:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMCreateResourcePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RAMResourceSharePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RAMAssociateResourceSharePermission",
```

```
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioAdminProjectUserRolePolicy

Descrição: Essa política do IAM concede a uma função do IAM acesso total ao AWS Glue Data Catalog (metadados) e ao Amazon S3 (dados reais) para operações de data lake, com acesso definido por conta e tags de função.

`SageMakerStudioAdminProjectUserRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioAdminProjectUserRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 09 de julho de 2025, 20:52 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminProjectUserRolePolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
```

```
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
      }
    },
    {
      "Sid" : "GlueCatalogDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
```

```
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
      }
    },
    {
      "Sid" : "DataAccessPermissionsForS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioBedrockAgentServiceRolePolicy

Descrição: permite que os agentes do Amazon Bedrock acessem modelos do Amazon Bedrock e outros recursos vinculados a um agente no SageMaker Studio.

`SageMakerStudioBedrockAgentServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioBedrockAgentServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 13 de fevereiro de 2025, 23:37 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockAgentServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
```

```
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockApplyGuardrailPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ApplyGuardrail",
      "Resource" : "arn:aws:bedrock:*:*:guardrail/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
```

```
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaInvokeFunctionInProjectPermissions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockRetrievePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:Retrieve",
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3GetObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAttributes",
        "s3:GetObjectAttributes"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "BedrockGuardrailKmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:guardrail-id" : "false"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioBedrockChatAgentUserRolePolicy

Descrição: Fornece acesso à configuração do aplicativo do agente de bate-papo Amazon Bedrock e ao agente Amazon Bedrock no SageMaker Studio.

`SageMakerStudioBedrockChatAgentUserRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioBedrockChatAgentUserRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 13 de fevereiro de 2025, 23:52 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockChatAgentUserRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockGetAgentAliasPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:GetAgentAlias",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/${aws:PrincipalTag/AgentId}/
${aws:PrincipalTag/AgentAliasId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeAgent",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/${aws:PrincipalTag/AgentId}/
${aws:PrincipalTag/AgentAliasId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockGetAndListAgentMetadataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
```

```
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgentVersions"
      ],
      "Resource" : "arn:aws:bedrock:*:*:agent/${aws:PrincipalTag/AgentId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3ListAppDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/AppDefinitionPath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AppDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "S3GetAppDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AppDefinitionPath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AppDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "S3ListDataSourcePermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/DataSourcePath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DataSourcePath" : ""
        }
      }
    },
    {
      "Sid" : "S3GetDataSourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/DataSourcePath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
```

```
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DataSourcePath" : ""
        }
      }
    },
    {
      "Sid" : "BedrockAgentKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:agent/${aws:PrincipalTag/AgentId}"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioBedrockEvaluationJobServiceRolePolicy

Descrição: permite que o Amazon Bedrock acesse modelos e conjuntos de dados do Amazon Bedrock para trabalhos de avaliação no Studio. SageMaker

`SageMakerStudioBedrockEvaluationJobServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioBedrockEvaluationJobServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 14 de fevereiro de 2025, 00:37 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockEvaluationJobServiceRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockEvaluationInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeModelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelInvocationJob",
        "bedrock:StopModelInvocationJob",
        "bedrock:GetProvisionedModelThroughput"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetBucketLocationPermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetBucketLocation",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
        }
      }
    },
    {
      "Sid" : "S3ListBucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
        },
```

```
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "S3EvaluationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/${aws:PrincipalTag/
AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "KmsDescribeKeyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioBedrockFlowServiceRolePolicy

Descrição: permite que o Amazon Bedrock Flows acesse modelos do Amazon Bedrock e outros recursos vinculados a um fluxo no SageMaker Studio.

`SageMakerStudioBedrockFlowServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioBedrockFlowServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 14 de fevereiro de 2025, 00:07 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockFlowServiceRolePolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockPromptPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:GetPrompt",
      "Resource" : "arn:aws:bedrock:*:*:prompt/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
```

```
      "Sid" : "BedrockKnowledgeBasePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:Retrieve",
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockGuardrailPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ApplyGuardrail",
      "Resource" : "arn:aws:bedrock:*:*:guardrail/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowBedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLambdaInvokeFunctionInProjectPermissions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
```

```
    {
      "Sid" : "AllowBedrockApplicationInferenceProfileAccessInProjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowBedrockInvokeModelAccessWithInferenceProfilePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeAgent",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
```

```
      "Sid" : "BedrockPromptKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock-prompts:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:prompt/*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockGuardrailKmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:guardrail-id" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockAgentKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:agent/*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioBedrockFunctionExecutionRolePolicy

Descrição: permite que o AWS Lambda acesse a configuração de um componente de função do Amazon Bedrock no SageMaker Studio.

`SageMakerStudioBedrockFunctionExecutionRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioBedrockFunctionExecutionRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 25 de fevereiro de 2025, 03:52 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockFunctionExecutionRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "KMSSameAccountBedrockViaSecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:
${aws:PrincipalAccount}:secret:amazon-bedrock*"
```

```
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy

Descrição: Fornece acesso para configurar armazenamentos vetoriais e bases de conhecimento do Amazon Bedrock no SageMaker Studio.

`SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 25 de fevereiro de 2025, 03:37 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OpenSearchServerlessPermissions",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aoss:collection" : "bedrock*"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetIngestionJob",
        "bedrock:ListIngestionJobs",
        "bedrock:StartIngestionJob"
      ],
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy

Descrição: permite que as bases de conhecimento do Amazon Bedrock acessem modelos e fontes de dados do Amazon Bedrock no SageMaker Studio.

`SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 25 de fevereiro de 2025, 02:52 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "OpenSearchServerlessPermissions",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aoss:collection" : "bedrock*"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : [
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "AccessDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
```

```
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "VectorStoresKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "VectorStoresKmsDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
```

```
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "NeptuneGraphDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:GetGraph",
        "neptune-graph:DeleteDataViaQuery",
        "neptune-graph:WriteDataViaQuery",
        "neptune-graph:ReadDataViaQuery"
      ],
      "Resource" : "arn:aws:neptune-graph:*:*:graph/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3VectorsDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3vectors:GetVectorBucket",
        "s3vectors:GetIndex",
        "s3vectors:PutVectors",
        "s3vectors:GetVectors",
        "s3vectors:ListVectors",
        "s3vectors:QueryVectors",
        "s3vectors:DeleteVectors"
      ],
      "Resource" : "arn:aws:s3vectors:*:*:bucket/amazon-bedrock-ide-${aws:PrincipalTag/
AmazonDataZoneProject}*",
```

```
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBaseKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:knowledge-base/*"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "SqlWorkbenchAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetSqlRecommendations",
        "sqlworkbench:PutSqlGenerationContext",
        "sqlworkbench:GetSqlGenerationContext",
        "sqlworkbench:DeleteSqlGenerationContext"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockGenerateQueryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioBedrockPromptUserRolePolicy

Descrição: Fornece acesso a um prompt do Amazon Bedrock e sua configuração no SageMaker Studio.

`SageMakerStudioBedrockPromptUserRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioBedrockPromptUserRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 14 de fevereiro de 2025, 00:22 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockPromptUserRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockPromptReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:GetPrompt",
      "Resource" : "arn:aws:bedrock:*:*:prompt/${aws:PrincipalTag/PromptId}:
${aws:PrincipalTag/PromptVersion}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
```

```
    {
      "Sid" : "S3ListPromptDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/PromptDefinitionPath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/PromptDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "S3GetPromptDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/PromptDefinitionPath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/PromptDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "BedrockPromptKmsPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock-prompts:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:prompt/${aws:PrincipalTag/PromptId}"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioDomainExecutionRolePolicy

Descrição: Essa política é usada pelo Amazon SageMaker Studio para catalogar, descobrir, governar, compartilhar e analisar dados no domínio do Amazon SageMaker Studio.

`SageMakerStudioDomainExecutionRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioDomainExecutionRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 20 de novembro de 2024, 21:56 UTC
- Horário editado: 12 de agosto de 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainExecutionRolePolicy`

Versão da política

Versão da política: v23 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZonePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:AssociateGovernedTerms",
        "datazone:BatchGetAttributesMetadata",
        "datazone:BatchPutAttributesMetadata",
        "datazone:BatchUpdateNotifications",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateConnection",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateRule",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetFilter",
        "datazone:DeleteAssetType",
        "datazone:DeleteConnection",
        "datazone:DeleteDataProduct",
        "datazone:DeleteDataSource",
        "datazone:DeleteDomainUnit",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
```

```
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteRule",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:DeleteTimeSeriesDataPoints",
        "datazone:DisassociateGovernedTerms",
        "datazone:GetAsset",
        "datazone:GetAssetFilter",
        "datazone:GetAssetType",
        "datazone:GetConnection",
        "datazone:GetCurrentEffectivePolicy",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDesignation",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetLineageNode",
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
        "datazone:GetProject",
        "datazone:GetRule",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUpdateEligibility",
        "datazone:GetUserProfile",
```

```
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetFilters",
        "datazone:ListAssetRevisions",
        "datazone:ListConnections",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDesignations",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListMetadataGenerationRuns",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListRules",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:ListWarehouseMetadata",
        "datazone:QueryGraph",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RemoveEntityOwner",
        "datazone:RemovePolicyGrant",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
```

```
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonQPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "q:GetIdentityMetadata",
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "SSMGetParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q/${aws:PrincipalTag/datazone-
domainId}*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/${aws:PrincipalTag/datazone-
domainId}/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetCodeConnectionsPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection",
        "codeconnections:GetHost",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "false"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "ListCodeConnectionsPermissionsStatement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codestar-connections:ListConnections",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "UseCodeConnectionsPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection",
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "false"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "ProjectProfilePermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GetProjectProfile",
        "datazone:ListProjectProfiles"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/*"
    },
    {
      "Sid" : "AccountPoolPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GetAccountPool",
        "datazone:ListAccountPools",
        "datazone:ListAccountsInAccountPool"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/*"
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioDomainServiceRolePolicy

Descrição: Função de serviço para ações em nível de domínio no portal que são executadas pelo Amazon SageMaker Studio.

`SageMakerStudioDomainServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioDomainServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 20 de novembro de 2024, 21:56 UTC
- Horário editado: 20 de novembro de 2024, 21:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SSMGetParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles/*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm.*.amazonaws.com",
          "kms:EncryptionContext:PARAMETER_ARN" : "arn:aws:ssm:*:*:parameter/amazon/
datazone/profiles*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioEMRContainersSystemNamespaceRolePolicy

Descrição: O Amazon SageMaker Studio cria funções do IAM para que usuários de projetos realizem ações de análise de dados, inteligência artificial e aprendizado de máquina, e usa essa política ao criar essas funções para definir as permissões relacionadas ao EMR.

`SageMakerStudioEMRContainersSystemNamespaceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioEMRContainersSystemNamespaceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 23 de outubro de 2025, 18:34 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRContainersSystemNamespaceRolePolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AssumeProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "TagSessionProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:TagSession"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LakeFormationAuthorizedCaller"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/LakeFormationAuthorizedCaller" : "EMR on EKS Engine",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
```

```
    {
      "Sid" : "SetContextProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "sts:RequestContextProviders" : [
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
          ]
        },
        "Null" : {
          "sts:RequestContextProviders" : "false"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioEMRInstanceRolePolicy

Descrição: O Amazon SageMaker Studio cria funções do IAM para que usuários de projetos realizem ações de análise de dados, inteligência artificial e aprendizado de máquina, e usa essa política ao criar essas funções para definir as permissões relacionadas ao EMR.

`SageMakerStudioEMRInstanceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioEMRInstanceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 27 de fevereiro de 2025, 00:22 UTC
- Horário editado: 01 de junho de 2026, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRInstanceRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessCertificateLocationS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/certificate_location/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : ""
        },
        "Null" : {
```

```
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessPatchingRPMsS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::default-env-blueprint-*/*",
        "arn:aws:s3:::awssmuscompute-blueprint-bucket-*/*",
        "arn:aws:s3:*:*:accesspoint/env-blueprint-accesspoint*",
        "arn:aws:s3:*:*:accesspoint/env-partner-blueprint-accesspoint*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : [
            "arn:aws:s3:*:*:accesspoint/env-blueprint-accesspoint",
            "arn:aws:s3:*:*:accesspoint/env-partner-blueprint-accesspoint"
          ]
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessBootstrapActionScriptS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AmazonDataZoneScopeName}/sys/emr/bootstrap-script/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneScopeName" : ""
        },
        "Null" : {
```

```
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRClusterLogUploadS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AmazonDataZoneScopeName}/sys/emr/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneScopeName" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRRuntimeRoleAssumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LakeFormationAuthorizedCaller"
          ]
        },
        "StringEquals" : {
```

```
          "iam:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EMRKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioEMRServiceRolePolicy

Descrição: O Amazon SageMaker Studio cria funções do IAM para que usuários de projetos realizem ações de análise de dados, inteligência artificial e aprendizado de máquina, e usa essa política ao criar essas funções para definir as permissões relacionadas ao EMR.

`SageMakerStudioEMRServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioEMRServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 31 de janeiro de 2025, 19:52 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRServiceRolePolicy`

Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PassRoleToEMREC2InstanceRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_
${aws:PrincipalTag/AmazonDataZoneProject}_${aws:PrincipalTag/
AmazonDataZoneEnvironment}",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneEnvironment" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreateInNetworkForSharedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        }
```

```
      }
    },
    {
      "Sid" : "EMRKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeKeyForLogPusherCMK",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioFullAccess

Descrição: Essa política fornece acesso total ao Amazon SageMaker Unified Studio por meio do console SageMaker de gerenciamento da Amazon.

`SageMakerStudioFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 28 de novembro de 2024, 00:06 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioFullAccess`

Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "iam:ListPolicies",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "secretsmanager:ListSecrets",
        "iam:ListUsers",
        "glue:GetDatabases",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codewhisperer:ListProfiles",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListFoundationModels",
        "bedrock:ListTagsForResource",
```

```
        "aoss:ListSecurityPolicies",
        "quicksight:DescribeAccountSubscription",
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BucketReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "ReadManagedBlueprintTemplatesStatement",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::default-env-blueprint-*/*",
        "arn:aws:s3:*:*:accesspoint/env-blueprint-accesspoint*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/env-blueprint-
accesspoint"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreateBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-datazone*",
```

```
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "ConfigureBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketCORS",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PutObjectStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RamCreateResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RamResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RamResourceReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations",
        "ram:ListResourceSharePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RamAssociateResourceSharePermissionStatement",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
```

```
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMGetPolicyStatement",
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
      "Sid" : "DataZoneTagOnCreateDomainProjectTags",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
```

```
            "AmazonDataZoneProject"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "DataZoneTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "CreateSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "ConnectionStatement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "codeconnections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "TagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:TagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:host/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "for-use-with-all-datazone-projects"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "UntagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UntagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:host/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "for-use-with-all-datazone-projects"
        }
      }
    },
```

```
    {
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
        "aoss:CreateSecurityPolicy"
      ],
      "Resource" : [
```

```
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "GetFoundationModelStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "GetInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*",
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ]
    },
    {
      "Sid" : "ApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "TagApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "ModelAccessUseCaseStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetUseCaseForModelAccess",
        "bedrock:PutUseCaseForModelAccess"
      ],
      "Resource" : [
```

```
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioProjectProvisioningRolePolicy

Descrição: O Amazon SageMaker Studio usa essa política para provisionar e gerenciar recursos em sua conta.

`SageMakerStudioProjectProvisioningRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioProjectProvisioningRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 20 de novembro de 2024, 21:58 UTC
- Horário editado: 22 de setembro de 2026, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioProjectProvisioningRolePolicy`

Versão da política

Versão da política: v83 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnMng",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:UpdateStack"
      ],
```

```
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnDelete",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Discovery",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "bedrock:ListEvaluationJobs",
        "cloudformation:ValidateTemplate",
        "codecommit:ListRepositories",
        "eks:DescribeCluster",
        "elasticmapreduce:CreateSecurityConfiguration",
        "elasticmapreduce:DeleteSecurityConfiguration",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "glue:DescribeConnectionType",
        "glue:ListConnectionTypes",
        "glue:*GlueIdentityCenterConfiguration",
        "iam:ListPolicies",
```

```
        "logs:DescribeLogGroups",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeDataShares",
        "redshift:DescribeDataSharesForConsumer",
        "redshift:GetResourcePolicy",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LFMng",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:DescribeResource",
        "lakeformation:*LakeFormationIdentityCenterConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DzTemplate",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "DzCfTemplate",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::amazon-sagemaker-cf-templates*/*"
    },
    {
      "Sid" : "DataZoneEnvironmentResources",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*Connection",
        "datazone:*DataSource",
        "datazone:*SubscriptionTarget"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CcCreate",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CreateRepository",
        "codecommit:TagResource"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CcDelete",
```

```
      "Effect" : "Allow",
      "Action" : [
        "codecommit:DeleteRepository",
        "codecommit:UntagResource",
        "codecommit:UpdateRepositoryEncryptionKey",
        "codecommit:PutRepositoryTriggers"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CcAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GetBranch",
        "codecommit:CreateCommit",
        "codecommit:GetRepository",
        "codecommit:GetFile"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CcKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "Null" : {
          "kms:EncryptionContext:aws:codecommit:id" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "codecommit.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetIamRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ]
    },
    {
      "Sid" : "IAMMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrockExecution*",
        "arn:aws:iam::*:role/BedrockStudio*",
        "arn:aws:iam::*:role/AmazonBedrockConsumptionRole*",
        "arn:aws:iam::*:role/AmazonBedrockEvaluation*"
      ],
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "IamDzMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "RoleCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "IamMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioProjectRoleMachineLearningPolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioEMRContainersSystemNamespaceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioEMRInstanceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2",
            "arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicyForSessions",
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole",
            "arn:aws:iam::aws:policy/AmazonSageMakerPartnerAppsFullAccess",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamMngAdmin",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
```

```
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioAdminProjectUserRolePolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioAdminIAMDefaultExecutionPolicy"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneAdminProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamMngBR",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonBedrock*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockAgentServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockChatAgentUserRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockFlowServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockFunctionExecutionRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockPromptUserRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockEvaluationJobServiceRolePolicy"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "IamTag",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/datazone_s3tables_*",
        "arn:aws:iam::*:role/datazone-partner-apps-*",
        "arn:aws:iam::*:role/datazone_redshift_serverless_admin_role_*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*",
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "BootstrappedServices",
            "AmazonBedrockManaged",
            "RedshiftDb*",
            "EnableAmazonBedrockPermissions",
            "EnableAmazonBedrockIDEPermissions",
            "EnableGlueWorkloadsPermissions",
            "EnableSageMakerMLWorkloadsPermissions",
            "DomainBucketName",
            "KmsKeyId",
            "DomainKmsKeyId",
            "DefaultGlueCatalogKmsKeyId",
            "LogGroupName",
            "RoleName",
            "vpcArn",
            "VpcId",
            "CreatedForUseWithSageMakerStudio",
            "SageMakerStudioQueryExecutionRole",
            "SageMakerSpacesDomainId"
          ]
        },
        "Null" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AdminProjectTagRoleMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneScopeName",
            "BootstrappedServices",
            "AmazonDataZoneAdminProject"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamTagBR",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonBedrock*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged",
            "DomainBucketName",
            "KmsKeyId",
            "AgentId",
```

```
            "AgentAliasId",
            "AppDefinitionPath",
            "DataSourcePath",
            "PromptId",
            "PromptVersion",
            "PromptDefinitionPath",
            "OpenSearchServerlessCollectionId"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamTagRS",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "RedshiftDb*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        }
      }
    },
    {
      "Sid" : "IamTagEMR",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_service_role_*",
        "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_*",
        "arn:aws:iam::*:role/datazone_emr_containers_system_namespace_role_*"
```

```
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "DataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "DomainBucketName",
            "KmsKeyId",
            "VpcId"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        }
      }
    },
    {
      "Sid" : "IamUntag",
      "Effect" : "Allow",
      "Action" : "iam:UntagRole",
      "Resource" : "arn:aws:iam::*:role/datazone_usr_role_*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "EnableAmazonBedrockIDEPermissions"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MngRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
```

```
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DzMngRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:UpdateAssumeRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/datazone_emr_*",
        "arn:aws:iam::*:role/datazone-partner-apps-*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/datazone_s3tables_*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamAttach",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        }
      }
```

```
    },
    {
      "Sid" : "IamDetach",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*"
      ]
    },
    {
      "Sid" : "DzMngPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "iam:CreatePolicy",
        "iam:ListPolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:CreatePolicyVersion",
        "iam:ListPolicyVersions",
        "iam:DeletePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*",
        "arn:aws:iam::*:policy/connector-manage-access-policy*",
        "arn:aws:iam::*:policy/SageMakerStudioQueryExecutionRolePolicy"
      ]
    },
    {
      "Sid" : "InstanceProfile",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/
datazone_emr_ec2_instance_profile_*"
    },
```

```
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com",
            "glue.amazonaws.com"
          ],
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "airflow.amazonaws.com",
            "athena.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForDZ",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "datazone.amazonaws.com",
            "sagemaker.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "PassRoleForGlue",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/datazone_s3tables_*",
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQueryExecution"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForEmr",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_service_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticmapreduce.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForEmrIP",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleToBR",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassRoleToLambda",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AossSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
observability.aoss.amazonaws.com/AWSServiceRoleForAmazonOpenSearchServerless",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "observability.aoss.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "GlueDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/s3tablescatalog",
        "arn:aws:glue:*:*:catalog/s3tablescatalog/*",
        "arn:aws:glue:*:*:database/s3tablescatalog/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnGlueDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueDbTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
```

```
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueDbDelete",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteDatabase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnTag",
```

```
      "Effect" : "Allow",
      "Action" : "glue:GetConnection",
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/datazone-glue-network-connection-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnMng",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection",
        "glue:DeleteConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/datazone-glue-network-connection-*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnections",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "AthenaConnection",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateDataCatalog"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GetConnection",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "ConnectionTag",
      "Effect" : "Allow",
      "Action" : [
        "athena:TagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "federated_athena*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "CreateConn",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngConnection",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteConnection",
        "glue:UpdateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngCatalogConn",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:DeleteConnection",
        "glue:UpdateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:EncryptionContext:glue_catalog_id" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "glue.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetDataCatalogEncSett",
      "Effect" : "Allow",
      "Action" : "glue:GetDataCatalogEncryptionSettings",
      "Resource" : "arn:aws:glue:*:*:catalog",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "Repo",
      "Effect" : "Allow",
      "Action" : [
        "serverlessrepo:GetCloudFormationTemplate",
        "serverlessrepo:CreateCloudFormationTemplate"
      ],
      "Resource" : [
        "arn:aws:serverlessrepo:*:*:applications/Athena*"
      ]
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/athena-federation-repository*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CfnChangeSet",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:transform/*"
      ]
    },
    {
```

```
      "Sid" : "LambdaMng",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaGet",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "athena.amazonaws.com",
            "cloudformation.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:TagResource"
```

```
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "aws:cloudformation:*",
            "federated_athena*",
            "lambda:createdBy"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaS3Get",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::awsserverlessrepo*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:CalledViaLast" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3List",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "Null" : {
          "s3:prefix" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3Create",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketCORS",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:DeleteBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "Cfn",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/athenafederatedcatalog*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/federated_athena_datacatalog" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "AthenaDC",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteDataCatalog",
        "athena:GetDataCatalog",
        "athena:UpdateDataCatalog"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQueryExecution",
        "arn:aws:iam::*:role/datazone_s3tables_*"
      ]
    },
```

```
    {
      "Sid" : "S3tPassConn",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/aws:s3tables"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "lakeformation:EnabledOnlyForMetaDataAccess" : "true"
        }
      }
    },
    {
      "Sid" : "GlueCatalogCreate",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueCatalogMgmt",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:UpdateCatalog",
        "glue:DeleteCatalog",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RSMng",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:DeleteNamespace",
        "redshift-serverless:DeleteWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshotcopyconfiguration/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftDataShare",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AssociateDataShareConsumer",
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:datashare:*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "redshift-serverless.amazonaws.com",
            "glue.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging"
      ],
      "Resource" : "arn:aws:s3:::redshift-staging-bucket-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "RedshiftTag",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "true"
        }
      }
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SGMng",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "SGRevoke",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "TagEc2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "aws:cloudformation:*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2Mng",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateLG",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
```

```
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LGRetention",
      "Effect" : "Allow",
      "Action" : "logs:PutRetentionPolicy",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngLG",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup",
        "logs:UntagResource",
        "logs:DeleteRetentionPolicy",
        "logs:GetDataProtectionPolicy",
        "logs:PutDataProtectionPolicy",
        "logs:DeleteDataProtectionPolicy",
        "logs:AssociateKmsKey",
        "logs:DisassociateKmsKey",
```

```
        "logs:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AthenaMng",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateWorkGroup",
        "athena:TagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "aws:cloudformation:*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AthenaWGDelete",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup",
```

```
        "athena:UpdateWorkGroup",
        "athena:UntagResource",
        "athena:GetWorkGroup"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftCreate",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagRSS",
      "Effect" : "Allow",
```

```
      "Action" : [
        "redshift-serverless:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/CreatedBy" : "false"
        }
      }
    },
    {
      "Sid" : "SecretProject",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "SecretAll",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "TagSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "CreatedBy"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/CreatedBy" : "false",
          "aws:TagKeys" : "false"
        }
      }
    },
    {
      "Sid" : "SecretKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SsoKms",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IdStoreKms",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateSLR",
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/emr-containers.amazonaws.com/
AWSServiceRoleForAmazonEMRContainers",
        "arn:aws:iam::*:role/aws-service-role/ops.athena.amazonaws.com/
AWSServiceRoleForAmazonAthena"
      ]
    },
    {
      "Sid" : "RssMng",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-serverless:GetCredentials",
        "redshift-serverless:UntagResource",
        "redshift-serverless:UpdateNamespace",
        "redshift-serverless:UpdateWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "RedshiftKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:redshift-serverless:arn" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "redshift-serverless.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BRSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagRsSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "Redshift",
            "aws:secretsmanager:*",
            "aws:redshift-serverless:*",
            "AmazonDataZone*",
            "datazone.rs.workgroup"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "TagSMD",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
        "arn:aws:sagemaker:*:*:mlflow-app/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagSMDForUpdate",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateDomain",
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
        "arn:aws:sagemaker:*:*:mlflow-app/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngSMD",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:UpdateDomain",
        "sagemaker:DeleteDomain"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:domain/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SMApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:AddTags",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeleteSpace",
      "Effect" : "Allow",
      "Action" : "sagemaker:DeleteSpace",
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "DeleteUserProfile",
      "Effect" : "Allow",
      "Action" : "sagemaker:DeleteUserProfile",
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrSCreate",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:CreateApplication",
        "emr-serverless:TagResource"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrSMng",
      "Effect" : "Allow",
```

```
      "Action" : [
        "emr-serverless:DeleteApplication",
        "emr-serverless:GetApplication",
        "emr-serverless:StopApplication",
        "emr-serverless:UpdateApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrSEc2Eni",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "ops.emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrSEc2Subnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "ops.emr-serverless.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "MLFlowCreate",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateMlflowTrackingServer",
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MLFlowDescribe",
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeMlflowTrackingServer",
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*"
    },
    {
      "Sid" : "MLFlowDelete",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteMlflowTrackingServer"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MLFlowServerlessCreate",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateMlflowApp"
```

```
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-app/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MLFlowServerlessDescribeDelete",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteMlflowApp",
        "sagemaker:DescribeMlflowApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-app/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AossMng",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetAccessPolicy",
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:UpdateAccessPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "aoss:collection" : "bedrock-ide-*",
          "aoss:index" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "MngAossPolicies",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
```

```
        "aoss:CreateSecurityPolicy",
        "aoss:DeleteSecurityPolicy",
        "aoss:UpdateSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "aoss:collection" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "GetAoss",
      "Effect" : "Allow",
      "Action" : "aoss:BatchGetCollection",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AossCollections",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateCollection",
        "aoss:UpdateCollection",
        "aoss:DeleteCollection",
        "aoss:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngNeptune",
      "Effect" : "Allow",
```

```
      "Action" : [
        "neptune-graph:CreateGraph",
        "neptune-graph:UpdateGraph",
        "neptune-graph:DeleteGraph",
        "neptune-graph:ListGraphs",
        "neptune-graph:GetGraph"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "S3VectorsMng",
      "Effect" : "Allow",
      "Action" : [
        "s3vectors:CreateVectorBucket",
        "s3vectors:DeleteVectorBucket",
        "s3vectors:ListVectorBuckets",
        "s3vectors:GetVectorBucket",
        "s3vectors:CreateIndex",
        "s3vectors:DeleteIndex",
        "s3vectors:ListIndexes",
        "s3vectors:GetIndex"
      ],
      "Resource" : "arn:aws:s3vectors:*:*:bucket/amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagNeptune",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:TagResource"
      ],
      "Resource" : "arn:aws:neptune-graph:*:*:graph/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
```

```
            "AmazonDataZone*",
            "AmazonBedrock*"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GetS3GenAI",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/dzd*/*/genAI/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetBR",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetGuardrail",
        "bedrock:GetPrompt",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BRMng",
```

```
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateAgent",
        "bedrock:UpdateAgent",
        "bedrock:PrepareAgent",
        "bedrock:DeleteAgent",
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentAlias",
        "bedrock:CreateAgentAlias",
        "bedrock:UpdateAgentAlias",
        "bedrock:DeleteAgentAlias",
        "bedrock:ListAgentActionGroups",
        "bedrock:GetAgentActionGroup",
        "bedrock:CreateAgentActionGroup",
        "bedrock:UpdateAgentActionGroup",
        "bedrock:DeleteAgentActionGroup",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:AssociateAgentKnowledgeBase",
        "bedrock:DisassociateAgentKnowledgeBase",
        "bedrock:UpdateAgentKnowledgeBase",
        "bedrock:CreateKnowledgeBase",
        "bedrock:UpdateKnowledgeBase",
        "bedrock:DeleteKnowledgeBase",
        "bedrock:ListDataSources",
        "bedrock:GetDataSource",
        "bedrock:CreateDataSource",
        "bedrock:UpdateDataSource",
        "bedrock:DeleteDataSource",
        "bedrock:ListIngestionJobs",
        "bedrock:GetIngestionJob",
        "bedrock:StartIngestionJob",
        "bedrock:StopIngestionJob",
        "bedrock:CreateGuardrail",
        "bedrock:UpdateGuardrail",
        "bedrock:DeleteGuardrail",
        "bedrock:CreateGuardrailVersion",
        "bedrock:CreatePrompt",
        "bedrock:UpdatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:CreateFlow",
        "bedrock:UpdateFlow",
        "bedrock:PrepareFlow",
```

```
        "bedrock:DeleteFlow",
        "bedrock:ListFlowAliases",
        "bedrock:GetFlowAlias",
        "bedrock:CreateFlowAlias",
        "bedrock:UpdateFlowAlias",
        "bedrock:DeleteFlowAlias",
        "bedrock:ListFlowVersions",
        "bedrock:GetFlowVersion",
        "bedrock:CreateFlowVersion",
        "bedrock:DeleteFlowVersion",
        "bedrock:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagBR",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : [
        "arn:aws:bedrock:*:*:agent-alias/*/TSTALIASID",
        "arn:aws:bedrock:*:*:flow/*/alias/TSTALIASID"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngBRJobs",
      "Effect" : "Allow",
      "Action" : "bedrock:BatchDeleteEvaluationJob",
      "Resource" : "*",
```

```
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BRLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:InvokeFunction",
        "lambda:DeleteFunction",
        "lambda:UpdateFunctionCode",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration",
        "lambda:ListVersionsByFunction",
        "lambda:PublishVersion",
        "lambda:GetPolicy",
        "lambda:AddPermission",
        "lambda:TagResource"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngBRLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:ListTags",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRClusterMng",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ModifyInstanceFleet",
        "elasticmapreduce:RunJobFlow",
        "elasticmapreduce:SetTerminationProtection",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "arn:aws:elasticmapreduce:*:*:cluster/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AirflowEnv",
      "Effect" : "Allow",
      "Action" : [
        "airflow:CreateEnvironment",
        "airflow:UpdateEnvironment",
        "airflow:DeleteEnvironment",
        "airflow:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "AirflowS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "VpcCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "ENICreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "KmsCreate",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "airflow.*.amazonaws.com",
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KmsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QueryRoleMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "QueryRoleCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
    },
    {
      "Sid" : "QueryRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioQueryExecutionRolePolicy"
          ]
        }
      }
    },
    {
      "Sid" : "TagQueryRole",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "CreatedForUseWithSageMakerStudio",
            "SageMakerStudioQueryExecutionRole"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "ListQueryPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
    },
    {
      "Sid" : "EMRCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrRoleCleanup",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListInstanceProfilesForRole",
        "iam:DeleteRolePolicy",
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone_emr_*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrInstanceCleanup",
      "Effect" : "Allow",
      "Action" : [
        "iam:RemoveRoleFromInstanceProfile",
```

```
        "iam:DeleteInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/
datazone_emr_ec2_instance_profile_*"
    },
    {
      "Sid" : "Scheduler",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListTagsForResource",
        "scheduler:GetScheduleGroup"
      ],
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ScheduleGroup",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:DeleteScheduleGroup",
        "scheduler:UntagResource"
      ],
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreateSchedule",
      "Effect" : "Allow",
      "Action" : "scheduler:CreateScheduleGroup",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
```

```
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagSchedule",
      "Effect" : "Allow",
      "Action" : "scheduler:TagResource",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeleteSchedule",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:DeleteSchedule"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule/SageMakerUnifiedStudio-*-*/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "MngQSFolder",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSource",
        "quicksight:CreateFolder",
        "quicksight:CreateFolderMembership",
        "quicksight:CreateVPCConnection",
        "quicksight:DeleteDataSource",
        "quicksight:DeleteFolder",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DeleteVPCConnection",
        "quicksight:ListFolderMembers",
        "quicksight:ListTagsForResource",
        "quicksight:UpdateDataSource",
        "quicksight:UpdateDataSourcePermissions",
        "quicksight:UpdateFolder",
        "quicksight:UpdateFolderPermissions",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QuickSightResources",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
```

```
        "quicksight:DescribeFolder",
        "quicksight:DescribeGroup",
        "quicksight:DescribeGroupMembership",
        "quicksight:DescribeUser",
        "quicksight:DescribeVPCConnection",
        "quicksight:ListTagsForResource",
        "quicksight:UpdateDashboardPermissions"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagQS",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:TagResource"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassRoleForQS",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQuickSightVPC",
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "quicksight.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PutRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/Managed.SageMaker*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.quicksight",
            "aws.codecommit"
          ]
        },
        "Null" : {
          "events:detail-type" : "false",
          "events:source" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "datazone.amazonaws.com",
          "events:detail-type" : [
            "AWS Service Event via CloudTrail",
            "CodeCommit Repository State Change"
          ]
        }
      }
    },
    {
      "Sid" : "MngEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutTargets",
        "events:RemoveTargets"
```

```
      ],
      "Resource" : "arn:aws:events:*:*:rule/Managed.SageMaker*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "RssAdmin",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGPerm",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccessGrantsInstance",
        "s3:CreateAccessGrantsInstance"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ResourceTagsUnTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:UntagResource",
```

```
        "neptune-graph:UntagResource",
        "quicksight:UntagResource",
        "glue:UntagResource",
        "airflow:UntagResource",
        "secretsmanager:UntagResource",
        "lambda:UntagResource",
        "emr-serverless:UntagResource",
        "elasticmapreduce:RemoveTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SSOMng",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:DeleteApplication",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso:PutApplicationAccessScope",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant",
        "sso:PutApplicationSessionConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "elasticmapreduce.amazonaws.com",
            "emr-containers.amazonaws.com",
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "ops.emr-serverless.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "EmrContainersMng",
      "Effect" : "Allow",
      "Action" : [
        "emr-containers:CreateManagedEndpoint",
        "emr-containers:CreateSecurityConfiguration",
        "emr-containers:CreateVirtualCluster",
        "emr-containers:DeleteManagedEndpoint",
        "emr-containers:DeleteSecurityConfiguration",
        "emr-containers:DeleteVirtualCluster",
        "emr-containers:DescribeSecurityConfiguration",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MngViaEmrContainers",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "eks:AssociateAccessPolicy",
        "eks:CreateAccessEntry",
        "eks:DisassociateAccessPolicy",
        "eks:DeleteAccessEntry",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "emr-containers.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioProjectRoleMachineLearningPolicy

Descrição: O Amazon SageMaker Studio cria funções do IAM para que os usuários de projetos realizem ações de análise de dados, inteligência artificial e aprendizado de máquina, e usa essa política ao criar essas funções para definir as permissões relacionadas SageMaker a.

`SageMakerStudioProjectRoleMachineLearningPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioProjectRoleMachineLearningPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 20 de novembro de 2024, 21:55 UTC
- Horário editado: 14 de setembro de 2026, 20:37 UTC

- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectRoleMachineLearningPolicy`

Versão da política

Versão da política: v44 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowManageSageMakerEniOnVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        },
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "sagemaker.amazonaws.com",
            "airflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManageSageMakerTrainingEniOnVpc",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        }
      }
    },
    {
      "Sid" : "AllowManageSageMakerEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerCreateVpcEndpointOnVpcId",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}",
      "Condition" : {
        "StringEquals" : {
          "ec2:VpcID" : "${aws:PrincipalTag/VpcId}"
        },
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerCreateVpcEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerDescribeVPCResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "glue:ListSessions",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeDhcpOptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSageMakerLogAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
      "Sid" : "SageMakerMlflowPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateMlflowTrackingServer",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerMlflowServerlessPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateMlflowApp",
        "sagemaker:CreatePresignedMlflowAppUrl",
        "sagemaker:DeleteMlflowApp",
        "sagemaker:DescribeMlflowApp",
        "sagemaker:UpdateMlflowApp",
        "sagemaker:CallMlflowAppApi"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-app/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "SageMakerBYOFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerBYOIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeImageVersion",
        "sagemaker:ListImageVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerStudioAppDescribeImageActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeImage"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:image/*"
    },
    {
      "Sid" : "SageMakerPipelinesSTSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerLogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
```

```
    },
    {
      "Sid" : "SageMakerCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateInferenceComponent",
        "sagemaker:CreatePipeline",
        "sagemaker:CreateInferenceRecommendationsJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerInferencePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StopTrainingJob",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchPutMetrics",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
```

```
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteInferenceComponent",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:InvokeEndpointWithResponseStream",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribeEndpoint"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerUpdateInferenceComponentRuntimeConfigAutoscalingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateInferenceComponentRuntimeConfig"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerDescribeUpdateDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeInferenceRecommendationsJob",
```

```
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:UpdatePipeline",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DeletePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopPipelineExecution",
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:RetryPipelineExecution",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerLineageSpecialPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateContext",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAction",
        "sagemaker:AddAssociation",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteArtifact"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerModelRegistryLineageSpecialPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:QueryLineage",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeContext"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:GetSearchSuggestions",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListModels",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListHubs",
        "sagemaker:ListPipelines",
        "sagemaker:ListContexts",
        "sagemaker:ListMlflowApps",
```

```
        "sagemaker:ListFeatureGroups",
        "scheduler:ListSchedules"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerSearchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Search"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "sagemaker:SearchVisibilityCondition/Tags.AmazonDataZoneProject/
EqualsIfExists" : "${aws:PrincipalTag/AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerListPermissionsTagRestricted",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListHubContents",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "SageMakerPublicHubReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHub",
        "sagemaker:DescribeHubContent",
        "sagemaker:ListHubContents"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub",
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerECRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*"
    },
    {
      "Sid" : "SageMakerECRGetAuthorizationTokenPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupGetPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupListPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupDeletePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerMLFlowModelRegistrationPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeModelPackageGroup"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:model-package-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioCreatePresignedDomainUrlForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "SageMakerStudioCreatePresignedDomainUrlForTaggedUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAppListActionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListApps",
        "sagemaker:ListDomains",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListSpaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerStudioAppDescribeDomainActionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAppDescribeJupyterLabAppActionPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ]
    },
    {
      "Sid" : "SageMakerStudioAppDescribeUserProfileActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAppDescribeTaggedUserProfilePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SMStudioAppDescribeSpaceActionPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:DescribeSpace"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*",
            "sagemaker*",
            "sm-jumpstart*",
            "endpoint-has-jumpstart-model"
          ]
        },
        "ForAllValues:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "sagemaker:shared-with:*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAllowCreatingDeletingOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile",
        "sagemaker:UpdateUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAllowCreatingDeletingTaggedOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile",
        "sagemaker:UpdateUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/*/
${aws:PrincipalTag/datazone:userId}"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceToOwnerUser",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/*/
${aws:PrincipalTag/datazone:userId}"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
```

```
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceAppsToOwnerUser",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStartSessionForSpaceRemoteConnection",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StartSession"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
```

```
    },
    {
      "Sid" : "PublishSagemakerMetric",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "/aws/sagemaker/*"
        }
      }
    },
    {
      "Sid" : "ManageSageMakerEndpointsAutoscalingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MutateSageMakerEndpointsAutoscalingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SSMPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
    },
    {
      "Sid" : "SageMakerJumpstartS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-*/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerCrossAccountPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:ListModelPackages",
        "sagemaker:CreateModel"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerListTagsRestrictionOnSharedResources",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerFeatureStorePermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*Feature*",
        "sagemaker:*Record"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerAutoScalingPermissionsWithserviceNamespace",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "sagemaker",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "SageMakerAutoScalingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerSLRForAutoScalingPermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "sagemaker.*.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "S3AGObjectRead",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGObjectWrite",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
```

```
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGBucketLevelReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:s3:arn"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "S3AGLocationManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateAccessGrantsLocation",
        "s3:DeleteAccessGrantsLocation",
        "s3:GetAccessGrantsLocation"
      ],
      "Resource" : [
        "arn:aws:s3:*:*:access-grants/default/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:accessGrantsLocationScope" : "s3://${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/"
        }
      }
    },
    {
      "Sid" : "S3AGPermissionManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateAccessGrant",
        "s3:DeleteAccessGrant"
      ],
      "Resource" : [
        "arn:aws:s3:*:*:access-grants/default/location/*",
        "arn:aws:s3:*:*:access-grants/default/grant/*"
      ],
      "Condition" : {
        "StringLike" : {
          "s3:accessGrantScope" : "s3://${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*"
        }
      }
    },
    {
      "Sid" : "CrossAccountS3AGResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "s3:AccessGrants"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountS3AGResourceSharingPolicyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutAccessGrantsInstanceResourcePolicy"
      ],
      "Resource" : "arn:aws:s3:*:*:access-grants/default",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGTaggingPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:TagResource",
        "s3:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:s3:*:*:access-grants/default/location/*",
        "arn:aws:s3:*:*:access-grants/default/grant/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ConsumerS3AGPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccessGrantsInstanceForPrefix",
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MLAccountDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:ListWorkflow*",
        "airflow-serverless:ListTask*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowServerlessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:CreateWorkflow",
        "airflow-serverless:DeleteWorkflow",
        "airflow-serverless:GetTaskInstance",
        "airflow-serverless:GetWorkflow",
        "airflow-serverless:GetWorkflowRun",
        "airflow-serverless:ListTagsForResource",
        "airflow-serverless:StartWorkflowRun",
        "airflow-serverless:StopWorkflowRun",
        "airflow-serverless:TagResource",
        "airflow-serverless:UntagResource",
        "airflow-serverless:UpdateWorkflow"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AirflowCloudwatchLogsActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/mwaa-serverless/${aws:PrincipalTag/
AmazonDataZoneDomain}-${aws:PrincipalTag/AmazonDataZoneProject}/*"
      ]
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless"
      ]
    },
    {
      "Sid" : "DataZoneUserPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GenerateCode",
        "datazone:CreateAsset*",
        "datazone:List*",
        "datazone:Search*",
        "datazone:*Message*",
        "datazone:*Conversation*",
        "datazone:*Cell*",
        "datazone:*Notebook*",
        "datazone:*Compute*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaSession",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetSessionEndpoint",
        "athena:GetResourceDashboard",
        "athena:TagResource"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SQLWorkBenchMLActionsWithResourceType",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioProjectUserRolePermissionsBoundary

Descrição: SageMaker A Amazon cria funções do IAM para que os usuários do Projects realizem ações de análise de dados, inteligência artificial e aprendizado de máquina, e usa essa política ao criar essas funções para definir o limite de suas permissões.

`SageMakerStudioProjectUserRolePermissionsBoundary` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioProjectUserRolePermissionsBoundary` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 20 de novembro de 2024, 21:57 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePermissionsBoundary`

Versão da política

Versão da política: v19 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DenyAllNonMatchingProjectTag",
      "Effect" : "Deny",
      "Action" : "*",
      "NotResource" : [
        "arn:*:sagemaker:*:*:model-package-group/*",
        "arn:*:sagemaker:*:*:model-package/*",
        "arn:*:glue:*:*:catalog/*",
        "arn:*:glue:*:*:database/*"
      ],
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:PrincipalTag/AmazonDataZoneProject" : "false",
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        },
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AmazonQChatPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataLakeS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SameAccountKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
```

```
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "redshift-serverless.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com",
            "ec2.*.amazonaws.com",
            "codecommit.*.amazonaws.com",
            "glue.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEmrEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SameAccountKMSManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:RevokeGrant",
        "kms:DescribeKey"
```

```
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com",
            "codecommit.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CrossAccountS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
```

```
        "s3:ListMultipartUploadParts",
        "s3:ListBucket",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CrossAccountKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "CrossAccountKMSManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListGrants",
```

```
        "kms:GetPublicKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "datazone.*.amazonaws.com"
          ]
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "DataZoneDescribeKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "datazone.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
```

```
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListDomainBucketFromAthenaFederatedCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
      ],
      "Condition" : {
        "ArnEquals" : {
          "lambda:SourceFunctionArn" :
 "arn:aws:lambda:*:*:function:athenafederatedcatalog_*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
```

```
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessCertificateS3LocationPermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/certificate_location/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagS3ObjectPermissionsForBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : "s3:PutObjectTagging",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
genAI/assets/evaluations/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "s3:RequestObjectTag/BasicValidationStatus" : [
```

```
            "valid",
            "invalid"
          ],
          "s3:RequestObjectTag/ContainsReferenceResponseForAllPrompts" : [
            "true",
            "false"
          ]
        },
        "ForAllValues:StringEquals" : {
          "s3:RequestObjectTagKeys" : [
            "BasicValidationStatus",
            "ContainsReferenceResponseForAllPrompts"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchDescribeLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:StartQuery",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/*",
        "arn:aws:logs:*:*:log-group:airflow*",
        "arn:aws:logs:*:*:log-group:datazone*"
      ]
```

```
    },
    {
      "Sid" : "CloudWatchStopQuery",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaPermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:UpdateNotebook",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
```

```
        "athena:DeleteNamedQuery",
        "athena:GetCalculationExecution",
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetNamedQuery",
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetSession",
        "athena:GetSessionStatus",
        "athena:GetWorkGroup",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "athena:ListQueryExecutions",
        "athena:ListTagsForResource",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DataZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:CreateConnection",
        "datazone:DeleteConnection",
        "datazone:GetConnection",
        "datazone:GetDomain",
        "datazone:GetDomainExecutionRoleCredentials",
```

```
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetProject",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListEnvironments",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListProjects",
        "datazone:UpdateConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
```

```
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCrawlerPermissions",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueGlobalTempDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueCatalogDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
```

```
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "GlueUnrestrictedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UseGlueStudio",
        "glue:ListSessions",
        "glue:StartCompletion",
        "glue:GetCompletion",
        "glue:GetGeneratedCode",
        "glue:GetTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GluePermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:CancelStatement",
        "glue:ListStatements",
        "glue:TagResource",
        "glue:UntagResource",
        "glue:DeleteSession",
        "glue:RunStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
```

```
        "glue:PutWorkflowRunProperties",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:ResumeWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:StartJobRun",
        "glue:CancelDataQualityRuleRecommendationRun",
        "glue:CancelDataQualityRulesetEvaluationRun",
        "glue:DeleteDataQualityRuleset",
        "glue:GetDataQualityModel",
        "glue:GetDataQualityModelResult",
        "glue:GetDataQualityResult",
        "glue:GetDataQualityRuleRecommendationRun",
        "glue:GetDataQualityRuleset",
        "glue:GetDataQualityRulesetEvaluationRun",
        "glue:ListDataQualityResults",
        "glue:ListDataQualityRuleRecommendationRuns",
        "glue:ListDataQualityRulesetEvaluationRuns",
        "glue:ListDataQualityRulesets",
        "glue:PublishDataQuality",
        "glue:PutDataQualityProfileAnnotation",
        "glue:PutDataQualityStatisticAnnotation",
        "glue:StartDataQualityRuleRecommendationRun",
        "glue:StartDataQualityRulesetEvaluationRun",
        "glue:UpdateDataQualityRuleset"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GlueCreateAndTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession",
```

```
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "sagemaker.amazonaws.com",
            "ec2.amazonaws.com",
            "emr-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsIAMSessionRestriction",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedshiftUnrestrictedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters",
        "sqlworkbench:PutTab",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:ListTabs",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource",
        "sqlworkbench:PassAccountSettings",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:CreateConnection",
```

```
        "sqlworkbench:PutQCustomContext",
        "sqlworkbench:GetQCustomContext",
        "sqlworkbench:DeleteQCustomContext",
        "sqlworkbench:GetQSqlRecommendations",
        "sqlworkbench:GetQSqlPromptQuotas",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftPermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift:DescribeTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AllowAccessExistingRedshiftCompute",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift:DescribeTags",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsForManagedWorkgroup",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:GetStagingBucketLocation",
        "redshift-serverless:GetManagedWorkgroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "redshift-data:glue-catalog-arn" : "arn:aws:glue:*:*:catalog/*"
        }
      }
    },
    {
      "Sid" : "RedshifServerlessCredentialsForManagedWorkgroup",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "redshift-data.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftExistingComputeConnectToCatalog",
      "Effect" : "Allow",
      "Action" : [
```

```
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "GenerativeAIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:*-model/*"
      ],
      "Condition" : {
        "Null" : {
```

```
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "ManageNetworkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateTags",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListImageVersions",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListContexts",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListModels",
```

```
            "sagemaker:ListModelPackages",
            "sagemaker:ListModelPackageGroups",
            "sagemaker:ListModelMetadata",
            "sagemaker:ListMlflowTrackingServers",
            "sagemaker:ListArtifacts",
            "sagemaker:ListAssociations",
            "sagemaker:ListHubContents",
            "sagemaker:ListHubs",
            "sagemaker:ListPipelineExecutionSteps",
            "sagemaker:ListPipelineExecutions",
            "sagemaker:ListPipelineParametersForExecution",
            "sagemaker:ListPipelines",
            "sagemaker:ListApps",
            "sagemaker:ListDomains",
            "sagemaker:ListUserProfiles",
            "sagemaker:ListSpaces",
            "sagemaker:ListTags",
            "sagemaker:DescribeMlflowTrackingServer",
            "sagemaker:DescribeImageVersion",
            "sagemaker:DescribeImage",
            "sagemaker:DescribeInferenceComponent",
            "sagemaker:DescribeEndpointConfig",
            "sagemaker:DescribeModel",
            "sagemaker:DescribeOptimizationJob",
            "sagemaker:DescribeEndpoint",
            "sagemaker:DescribeInferenceRecommendationsJob",
            "sagemaker:DescribeModelPackage",
            "sagemaker:DescribeModelPackageGroup",
            "sagemaker:DescribePipeline",
            "sagemaker:DescribePipelineExecution",
            "sagemaker:DescribePipelineDefinitionForExecution",
            "sagemaker:DescribeHyperParameterTuningJob",
            "sagemaker:DescribeAutoMLJob",
            "sagemaker:DescribeAutoMLJobV2",
            "sagemaker:DescribeProcessingJob",
            "sagemaker:DescribeTrainingJob",
            "sagemaker:DescribeAction",
            "sagemaker:DescribeArtifact",
            "sagemaker:DescribeTrialComponent",
            "sagemaker:DescribeContext",
            "sagemaker:DescribeDomain",
            "sagemaker:DescribeApp",
            "sagemaker:DescribeUserProfile",
            "sagemaker:DescribeSpace",
```

```
        "sagemaker:AddTags",
        "sagemaker:AddAssociation",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteUserProfile",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:DeleteApp",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateSpace",
        "sagemaker:CreateApp",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreatePipeline",
        "sagemaker:CreateContext",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAction",
        "sagemaker:CreateInferenceComponent",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchPutMetrics",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
```

```
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteInferenceComponent",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:InvokeEndpointWithResponseStream",
        "sagemaker:QueryLineage",
        "sagemaker:UpdatePipeline",
        "sagemaker:DeletePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopPipelineExecution",
        "sagemaker:RetryPipelineExecution",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:Search",
        "sagemaker:UpdateMlflowTrackingServer",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker:ListPartnerApps",
        "sagemaker:CreatePartnerAppPresignedUrl",
        "sagemaker:DescribePartnerApp",
        "sagemaker:CallPartnerAppApi",
        "sagemaker-mlflow:AccessUI",
        "sagemaker-mlflow:CreateExperiment",
        "sagemaker-mlflow:SearchExperiments",
        "sagemaker-mlflow:GetExperiment",
        "sagemaker-mlflow:GetExperimentByName",
        "sagemaker-mlflow:DeleteExperiment",
        "sagemaker-mlflow:RestoreExperiment",
        "sagemaker-mlflow:UpdateExperiment",
        "sagemaker-mlflow:CreateRun",
        "sagemaker-mlflow:DeleteRun",
        "sagemaker-mlflow:RestoreRun",
        "sagemaker-mlflow:GetRun",
        "sagemaker-mlflow:LogMetric",
        "sagemaker-mlflow:LogBatch",
```

```
        "sagemaker-mlflow:LogModel",
        "sagemaker-mlflow:LogInputs",
        "sagemaker-mlflow:SetExperimentTag",
        "sagemaker-mlflow:SetTag",
        "sagemaker-mlflow:DeleteTag",
        "sagemaker-mlflow:LogParam",
        "sagemaker-mlflow:GetMetricHistory",
        "sagemaker-mlflow:SearchRuns",
        "sagemaker-mlflow:ListArtifacts",
        "sagemaker-mlflow:UpdateRun",
        "sagemaker-mlflow:CreateRegisteredModel",
        "sagemaker-mlflow:GetRegisteredModel",
        "sagemaker-mlflow:RenameRegisteredModel",
        "sagemaker-mlflow:UpdateRegisteredModel",
        "sagemaker-mlflow:DeleteRegisteredModel",
        "sagemaker-mlflow:GetLatestModelVersions",
        "sagemaker-mlflow:CreateModelVersion",
        "sagemaker-mlflow:GetModelVersion",
        "sagemaker-mlflow:UpdateModelVersion",
        "sagemaker-mlflow:DeleteModelVersion",
        "sagemaker-mlflow:SearchModelVersions",
        "sagemaker-mlflow:GetDownloadURIForModelVersionArtifacts",
        "sagemaker-mlflow:TransitionModelVersionStage",
        "sagemaker-mlflow:SearchRegisteredModels",
        "sagemaker-mlflow:SetRegisteredModelTag",
        "sagemaker-mlflow:DeleteRegisteredModelTag",
        "sagemaker-mlflow:DeleteModelVersionTag",
        "sagemaker-mlflow:DeleteRegisteredModelAlias",
        "sagemaker-mlflow:SetRegisteredModelAlias",
        "sagemaker-mlflow:GetModelVersionByAlias",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:DescribeImages",
        "elasticfilesystem:DescribeMountTargets",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath",
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerSLRForAutoScalingPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ComputePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "sts:GetCallerIdentity",
        "sts:TagSession",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRunAttempts",
        "emr-serverless:ListJobRuns",
        "emr-serverless:StartApplication",
        "emr-serverless:StartJobRun",
        "emr-serverless:StopApplication",
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "elasticmapreduce:ListReleaseLabels",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:DescribePersistentAppUI",
        "elasticmapreduce:GetPersistentAppUIPresignedURL",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sts:AssumeRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "SetSourceIdentityForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "AllowListSecrets",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "ComputePermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
```

```
        "redshift-data:ListTables",
        "elasticmapreduce:GetClusterSessionCredentials",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetOnClusterAppUIPresignedURL",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:TerminateJobFlows",
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DataLakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCommitPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGetCommits",
        "codecommit:BatchGetPullRequests",
        "codecommit:BatchGetRepositories",
        "codecommit:BatchDescribeMergeConflicts",
        "codecommit:CreateBranch",
        "codecommit:CreateCommit",
        "codecommit:CreatePullRequest",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:DescribeMergeConflicts",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetBlob",
        "codecommit:GetBranch",
```

```
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetFile",
        "codecommit:GetFolder",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
        "codecommit:ListBranches",
        "codecommit:ListFileCommitHistory",
        "codecommit:ListPullRequests",
        "codecommit:ListTagsForResource",
        "codecommit:MergeBranchesByFastForward",
        "codecommit:MergeBranchesBySquash",
        "codecommit:MergeBranchesByThreeWay",
        "codecommit:MergePullRequestByFastForward",
        "codecommit:MergePullRequestBySquash",
        "codecommit:MergePullRequestByThreeWay",
        "codecommit:UpdateComment",
        "codecommit:UpdateDefaultBranch",
        "codecommit:UpdatePullRequestApprovalRuleContent",
        "codecommit:UpdatePullRequestApprovalState",
        "codecommit:UpdatePullRequestDescription",
        "codecommit:UpdatePullRequestStatus",
        "codecommit:UpdatePullRequestTitle",
        "codecommit:UpdateRepositoryDescription",
        "codecommit:PostCommentForComparedCommit",
```

```
        "codecommit:PostCommentForPullRequest",
        "codecommit:PostCommentReply",
        "codecommit:PutCommentReaction",
        "codecommit:PutFile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EMRServicePermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreatePlacementGroup",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeletePlacementGroup",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
```

```
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModelRegistryResourceGroupGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModelRegistryResourceGroupMutatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        }
      }
    },
    {
      "Sid" : "ModelRegistryBedRockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessAossCollectionsForBedrock",
      "Effect" : "Allow",
```

```
      "Action" : "aoss:APIAccessAll",
      "Resource" : "*"
    },
    {
      "Sid" : "AccessBedrockResources",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:InvokeAgent",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
        "bedrock:ListIngestionJobs",
        "bedrock:ApplyGuardrail",
        "bedrock:ListPrompts",
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
        "bedrock:GetEvaluationJob",
        "bedrock:CreateEvaluationJob",
        "bedrock:StopEvaluationJob",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:ListTagsForResource",
        "bedrock:CreateAgentAlias",
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentVersions",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:GetAgentAlias",
        "bedrock:UpdateAgentAlias"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
```

```
      }
    },
    {
      "Sid" : "CreateEvaluationJobForFoundationModel",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*"
      ]
    },
    {
      "Sid" : "InvokeBedrockInlineAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "ListBedrockEvaluationJobPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListEvaluationJobs",
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "TagBedrockResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBaseDataIngestionKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "kms:ViaService" : "true",
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
        }
      }
    },
    {
      "Sid" : "AccessSecretPermissionsForBedrockApp",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "InvokeFunctionPermissionsForBedrockApp",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GetDataZoneEnvironmentCfnStackPermissionsForBedrockAppExport",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "MWAAPermissions",
      "Effect" : "Allow",
      "Action" : [
        "airflow:ListEnvironments",
        "airflow:GetEnvironment",
        "airflow:UpdateEnvironment",
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AirflowS3GetAccountPublicAccessBlock",
      "Effect" : "Allow",
      "Action" : "s3:GetAccountPublicAccessBlock",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
    },
    {
      "Sid" : "SQSPermissionsForMWAA",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Resource" : "arn:aws:sqs:*:*:airflow-celery-*"
    },
    {
      "Sid" : "FederatedDataConnectionGlueSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueConnectionAccessForFederatedDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListConnectionTypes",
        "glue:DescribeConnectionType"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueEntitiesAccessForFederatedDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListEntities",
        "glue:DescribeEntity",
        "glue:GetEntityRecords"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretAccessForForUseWithAllDataZoneProjectsSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "AccessForDynamoDbConnections",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "InvokeFunctionPermissionsForAthenaCatalogLambda",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceTag/federated_athena_datacatalog" : "true"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketForQueryExecutionRolePermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3PermissionsForAthenaCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::redshift-staging-bucket-*/*",
        "arn:aws:s3:::redshift-staging-bucket-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "GetS3ObjectForQueryExecutionRolePermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*/dzd_*/*/dev/sys/athena/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "NotDeniedOperations",
      "Effect" : "Deny",
      "NotAction" : [
        "airflow:CreateWebLoginToken",
        "airflow:GetEnvironment",
        "airflow:InvokeRestApi",
        "airflow:ListEnvironments",
        "airflow:UpdateEnvironment",
        "aoss:APIAccessAll",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetCalculationExecution",
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
```

```
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetSession",
        "athena:GetSessionStatus",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "bedrock:ApplyGuardrail",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:CreateAgentAlias",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreatePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeletePrompt",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:GetEvaluationJob",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestionJob",
        "bedrock:GetPrompt",
```

```
        "bedrock:InvokeAgent",
        "bedrock:InvokeFlow",
        "bedrock:InvokeInlineAgent",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgentVersions",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFoundationModels",
        "bedrock:ListIngestionJobs",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "bedrock:Retrieve",
        "bedrock:RetrieveAndGenerate",
        "bedrock:StartIngestionJob",
        "bedrock:StopEvaluationJob",
        "bedrock:TagResource",
        "bedrock:UpdateAgentAlias",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchDescribeMergeConflicts",
        "codecommit:BatchGetCommits",
        "codecommit:BatchGetPullRequests",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateBranch",
        "codecommit:CreateCommit",
        "codecommit:CreatePullRequest",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:DescribeMergeConflicts",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetBlob",
        "codecommit:GetBranch",
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
```

```
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetFile",
        "codecommit:GetFolder",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
        "codecommit:ListBranches",
        "codecommit:ListFileCommitHistory",
        "codecommit:ListPullRequests",
        "codecommit:ListTagsForResource",
        "codecommit:MergeBranchesByFastForward",
        "codecommit:MergeBranchesBySquash",
        "codecommit:MergeBranchesByThreeWay",
        "codecommit:MergePullRequestByFastForward",
        "codecommit:MergePullRequestBySquash",
        "codecommit:MergePullRequestByThreeWay",
        "codecommit:PostCommentForComparedCommit",
        "codecommit:PostCommentForPullRequest",
        "codecommit:PostCommentReply",
        "codecommit:PutCommentReaction",
        "codecommit:PutFile",
        "codecommit:UpdateComment",
        "codecommit:UpdateDefaultBranch",
        "codecommit:UpdatePullRequestApprovalRuleContent",
        "codecommit:UpdatePullRequestApprovalState",
        "codecommit:UpdatePullRequestDescription",
        "codecommit:UpdatePullRequestStatus",
        "codecommit:UpdatePullRequestTitle",
```

```
        "codecommit:UpdateRepositoryDescription",
        "codewhisperer:GenerateRecommendations",
        "datazone:CreateConnection",
        "datazone:DeleteConnection",
        "datazone:GetConnection",
        "datazone:GetDomain",
        "datazone:GetDomainExecutionRoleCredentials",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetProject",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironments",
        "datazone:ListProjects",
        "datazone:UpdateConnection",
        "dynamodb:BatchGetItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:Scan",
        "dynamodb:Query",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeEndpoints",
        "dynamodb:DescribeExport",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeImport",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetItem",
        "dynamodb:GetRecords",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListImports",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "dynamodb:PutItem",
```

```
        "dynamodb:PartiQLSelect",
        "dynamodb:PartiQLInsert",
        "dynamodb:PartiQLUpdate",
        "dynamodb:PartiQLDelete",
        "dynamodb:UpdateItem",
        "dynamodb:UpdateGlobalTable",
        "dynamodb:UpdateTable",
        "ec2:AttachNetworkInterface",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreatePlacementGroup",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface",
```

```
        "ec2:ModifyInstanceAttribute",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "elasticfilesystem:DescribeMountTargets",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribePersistentAppUI",
        "elasticmapreduce:GetClusterSessionCredentials",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetOnClusterAppUIPresignedURL",
        "elasticmapreduce:GetPersistentAppUIPresignedURL",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListReleaseLabels",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:TerminateJobFlows",
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRunAttempts",
        "emr-serverless:ListJobRuns",
        "emr-serverless:StartApplication",
        "emr-serverless:StartJobRun",
        "emr-serverless:StopApplication",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
```

```
            "glue:CancelDataQualityRuleRecommendationRun",
            "glue:CancelDataQualityRulesetEvaluationRun",
            "glue:CancelStatement",
            "glue:CreateBlueprint",
            "glue:CreateDatabase",
            "glue:CreateDataQualityRuleset",
            "glue:CreateJob",
            "glue:CreatePartition",
            "glue:CreatePartitionIndex",
            "glue:CreateSession",
            "glue:CreateTable",
            "glue:CreateWorkflow",
            "glue:DeleteBlueprint",
            "glue:DeleteColumnStatisticsForPartition",
            "glue:DeleteColumnStatisticsForTable",
            "glue:DeleteDatabase",
            "glue:DeleteDataQualityRuleset",
            "glue:DeleteJob",
            "glue:DeletePartition",
            "glue:DeletePartitionIndex",
            "glue:DeleteSession",
            "glue:DeleteTable",
            "glue:DeleteTableVersion",
            "glue:DeleteWorkflow",
            "glue:DescribeConnectionType",
            "glue:DescribeEntity",
            "glue:GetCatalog",
            "glue:GetCatalogImportStatus",
            "glue:GetCatalogs",
            "glue:GetClassifier",
            "glue:GetClassifiers",
            "glue:GetColumnStatisticsForPartition",
            "glue:GetColumnStatisticsForTable",
            "glue:GetColumnStatisticsTaskRun",
            "glue:GetColumnStatisticsTaskRuns",
            "glue:GetCompletion",
            "glue:GetConnection",
            "glue:GetConnections",
            "glue:GetDashboardUrl",
            "glue:GetDatabase",
            "glue:GetDatabases",
            "glue:GetDataQualityModel",
            "glue:GetDataQualityModelResult",
            "glue:GetDataQualityResult",
```

```
        "glue:GetDataQualityRuleRecommendationRun",
        "glue:GetDataQualityRuleset",
        "glue:GetDataQualityRulesetEvaluationRun",
        "glue:GetEntityRecords",
        "glue:GetGeneratedCode",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTags",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions",
        "glue:ListConnectionTypes",
        "glue:ListCrawls",
        "glue:ListDataQualityResults",
        "glue:ListDataQualityRuleRecommendationRuns",
        "glue:ListDataQualityRulesetEvaluationRuns",
        "glue:ListDataQualityRulesets",
        "glue:ListEntities",
        "glue:ListSessions",
        "glue:ListStatements",
        "glue:ListTableOptimizerRuns",
        "glue:NotifyEvent",
        "glue:PassConnection",
        "glue:PublishDataQuality",
        "glue:PutDataQualityProfileAnnotation",
        "glue:PutDataQualityStatisticAnnotation",
        "glue:PutWorkflowRunProperties",
        "glue:ResumeWorkflowRun",
        "glue:RunStatement",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCompletion",
        "glue:StartDataQualityRuleRecommendationRun",
        "glue:StartDataQualityRulesetEvaluationRun",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopSession",
```

```
        "glue:StopWorkflowRun",
        "glue:TagResource",
        "glue:UntagResource",
        "glue:UpdateBlueprint",
        "glue:UpdateCatalog",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateDataQualityRuleset",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow",
        "glue:UseGlueStudio",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole",
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:GetPublicKey",
        "kms:ListAliases",
        "kms:ListGrants",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:RevokeGrant",
        "lakeformation:GetDataAccess",
        "lambda:InvokeFunction",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:GetQueryResults",
        "logs:PutLogEvents",
        "logs:StartQuery",
        "logs:StopQuery",
        "pricing:GetProducts",
```

```
        "q:SendMessage",
        "q:StartConversation",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStagingBucketLocation",
        "redshift-data:GetStatementResult",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListStatements",
        "redshift-data:ListTables",
        "redshift-serverless:GetCredentials",
        "redshift-serverless:GetManagedWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters",
        "redshift:DescribeTags",
        "redshift:GetClusterCredentialsWithIAM",
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources",
        "resource-groups:Tag",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketLocation",
        "s3:GetEncryptionConfiguration",
        "s3:GetObject*",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:PutObjectTagging",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "sagemaker-mlflow:AccessUI",
```

```
            "sagemaker-mlflow:CreateExperiment",
            "sagemaker-mlflow:CreateModelVersion",
            "sagemaker-mlflow:CreateRegisteredModel",
            "sagemaker-mlflow:CreateRun",
            "sagemaker-mlflow:DeleteExperiment",
            "sagemaker-mlflow:DeleteModelVersion",
            "sagemaker-mlflow:DeleteModelVersionTag",
            "sagemaker-mlflow:DeleteRegisteredModel",
            "sagemaker-mlflow:DeleteRegisteredModelAlias",
            "sagemaker-mlflow:DeleteRegisteredModelTag",
            "sagemaker-mlflow:DeleteRun",
            "sagemaker-mlflow:DeleteTag",
            "sagemaker-mlflow:GetDownloadURIForModelVersionArtifacts",
            "sagemaker-mlflow:GetExperiment",
            "sagemaker-mlflow:GetExperimentByName",
            "sagemaker-mlflow:GetLatestModelVersions",
            "sagemaker-mlflow:GetMetricHistory",
            "sagemaker-mlflow:GetModelVersion",
            "sagemaker-mlflow:GetModelVersionByAlias",
            "sagemaker-mlflow:GetRegisteredModel",
            "sagemaker-mlflow:GetRun",
            "sagemaker-mlflow:ListArtifacts",
            "sagemaker-mlflow:LogBatch",
            "sagemaker-mlflow:LogInputs",
            "sagemaker-mlflow:LogMetric",
            "sagemaker-mlflow:LogModel",
            "sagemaker-mlflow:LogParam",
            "sagemaker-mlflow:RenameRegisteredModel",
            "sagemaker-mlflow:RestoreExperiment",
            "sagemaker-mlflow:RestoreRun",
            "sagemaker-mlflow:SearchExperiments",
            "sagemaker-mlflow:SearchModelVersions",
            "sagemaker-mlflow:SearchRegisteredModels",
            "sagemaker-mlflow:SearchRuns",
            "sagemaker-mlflow:SetExperimentTag",
            "sagemaker-mlflow:SetRegisteredModelAlias",
            "sagemaker-mlflow:SetRegisteredModelTag",
            "sagemaker-mlflow:SetTag",
            "sagemaker-mlflow:TransitionModelVersionStage",
            "sagemaker-mlflow:UpdateExperiment",
            "sagemaker-mlflow:UpdateModelVersion",
            "sagemaker-mlflow:UpdateRegisteredModel",
            "sagemaker-mlflow:UpdateRun",
            "sagemaker:AddAssociation",
```

```
        "sagemaker:AddTags",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CallPartnerAppApi",
        "sagemaker:CreateAction",
        "sagemaker:CreateApp",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:CreateContext",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateInferenceComponent",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreatePartnerAppPresignedUrl",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateSpace",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteInferenceComponent",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteSpace",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DescribeAction",
```

```
        "sagemaker:DescribeApp",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribePartnerApp",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:InvokeEndpointWithResponseStream",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListContexts",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListHubContents",
        "sagemaker:ListHubs",
        "sagemaker:ListHyperParameterTuningJobs",
```

```
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModels",
        "sagemaker:ListPartnerApps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListSpaces",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListUserProfiles",
        "sagemaker:QueryLineage",
        "sagemaker:RetryPipelineExecution",
        "sagemaker:Search",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "sagemaker:UpdateMlflowTrackingServer",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateSpace",
        "sagemaker:UpdateTrainingJob",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
```

```
        "secretsmanager:ListSecrets",
        "secretsmanager:PutSecretValue",
        "sqlworkbench:CreateConnection",
        "sqlworkbench:DeleteQCustomContext",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource",
        "sqlworkbench:GetQCustomContext",
        "sqlworkbench:GetQSqlPromptQuotas",
        "sqlworkbench:GetQSqlRecommendations",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:ListTabs",
        "sqlworkbench:PassAccountSettings",
        "sqlworkbench:PutQCustomContext",
        "sqlworkbench:PutTab",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath",
        "sts:AssumeRole",
        "sts:GetCallerIdentity",
        "sts:SetSourceIdentity",
        "sts:TagSession",
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioProjectUserRolePolicy

Descrição: O Amazon SageMaker Studio cria funções do IAM para que usuários de projetos realizem ações de análise de dados, inteligência artificial e aprendizado de máquina, e usa essa política ao criar essas funções para definir as permissões.

`SageMakerStudioProjectUserRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioProjectUserRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 20 de novembro de 2024, 21:59 UTC
- Horário editado: 27 de agosto de 2026, 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePolicy`

Versão da política

Versão da política: v75 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeCommit",
```

```
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGetCommits",
        "codecommit:BatchGetPullRequests",
        "codecommit:BatchGetRepositories",
        "codecommit:BatchDescribeMergeConflicts",
        "codecommit:CreateBranch",
        "codecommit:CreateCommit",
        "codecommit:CreatePullRequest",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:DescribeMergeConflicts",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetBlob",
        "codecommit:GetBranch",
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetFile",
        "codecommit:GetFolder",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
        "codecommit:ListBranches",
        "codecommit:ListFileCommitHistory",
        "codecommit:ListPullRequests",
        "codecommit:ListTagsForResource",
```

```
        "codecommit:MergeBranchesByFastForward",
        "codecommit:MergeBranchesBySquash",
        "codecommit:MergeBranchesByThreeWay",
        "codecommit:MergePullRequestByFastForward",
        "codecommit:MergePullRequestBySquash",
        "codecommit:MergePullRequestByThreeWay",
        "codecommit:UpdateComment",
        "codecommit:UpdateDefaultBranch",
        "codecommit:UpdatePullRequestApprovalRuleContent",
        "codecommit:UpdatePullRequestApprovalState",
        "codecommit:UpdatePullRequestDescription",
        "codecommit:UpdatePullRequestStatus",
        "codecommit:UpdatePullRequestTitle",
        "codecommit:UpdateRepositoryDescription",
        "codecommit:PostCommentForComparedCommit",
        "codecommit:PostCommentForPullRequest",
        "codecommit:PostCommentReply",
        "codecommit:PutCommentReaction",
        "codecommit:PutFile"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CodeCommitKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:codecommit:id" : "false"
        },
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "codecommit.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CodeWhisperer",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGlueCreateEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "true"
        },
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueENIonSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueENIonSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws-glue-service-resource" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueEniOnInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeGlueEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueKernelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "glue:ListSessions",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCreateAndTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:TagResource"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "ProjectUserTag*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
```

```
      }
    },
    {
      "Sid" : "GlueTagSessionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*"
          ]
        },
        "ForAllValues:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:*Session*",
        "glue:*Statement*",
        "glue:GetDashboardUrl",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
```

```
        "glue:PutWorkflowRunProperties",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:ResumeWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:StartJobRun",
        "glue:*DataQuality*",
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:BatchGetJobs",
        "glue:GetJob"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueDQ",
      "Effect" : "Allow",
      "Action" : "glue:ListDataQuality*",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "GlueDQVetl",
      "Effect" : "Allow",
      "Action" : [
        "glue:*DataQuality*"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:dataQualityRuleset/dq_etl_ruleset_${aws:PrincipalTag/
AmazonDataZoneProject}_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "GlueListJobs",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListJobs"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueVisualETL",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetGeneratedCode"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCompletions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
```

```
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*",
        "arn:aws:glue:*:*:job/*"
      ]
    },
    {
      "Sid" : "GlueJobRunnerSessionLog",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws-glue/*"
    },
    {
      "Sid" : "EC2TagsForGlue",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "aws-glue-*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueKmsPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/${aws:PrincipalTag/DefaultGlueCatalogKmsKeyId}",
        "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}"
      ],
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:glue_catalog_id" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "glue.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EMRS",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "emr-serverless:GetApplication",
        "emr-serverless:StartApplication",
        "emr-serverless:StopApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:*Session*",
        "emr-serverless:GetResourceDashboard",
        "emr-serverless:TagResource",
        "emr-serverless:StartJobRun"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "AirflowActionsForTaggedEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "airflow:UpdateEnvironment"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AirflowListEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "airflow:ListEnvironments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowUiApiAccess",
      "Effect" : "Allow",
      "Action" : [
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
      ],
      "Resource" : [
        "arn:aws:airflow:*:*:role/DataZoneMWAAEnv-${aws:PrincipalTag/
AmazonDataZoneDomain}-${aws:PrincipalTag/AmazonDataZoneProject}-${aws:PrincipalTag/
AmazonDataZoneScopeName}/User"
      ]
    },
    {
      "Sid" : "AirflowCloudwatchLogsActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogStreams",
```

```
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:airflow-DataZoneMWAAEnv-${aws:PrincipalTag/
AmazonDataZoneDomain}-${aws:PrincipalTag/AmazonDataZoneProject}-${aws:PrincipalTag/
AmazonDataZoneScopeName}-*"
      ]
    },
    {
      "Sid" : "AirflowCloudwatchActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "AmazonMWAA"
        }
      }
    },
    {
      "Sid" : "GlueJobCWPutMetricActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "Glue",
            "AWS/Glue",
            "Glue Data Quality"
          ]
        }
      }
    },
    {
      "Sid" : "AirflowS3GetAccountPublicAccessBlock",
```

```
      "Effect" : "Allow",
      "Action" : "s3:GetAccountPublicAccessBlock",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowSqsActions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:airflow-celery-*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketPublicAccessBlock"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "DataLakeS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataLakeCrossAccountS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataLakeCrossAccountKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:GetPublicKey",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "XAcctKmsDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:s3:arn"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : [
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DomainBucketName" : ""
```

```
        }
      }
    },
    {
      "Sid" : "AirflowListDomainS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
        }
      }
    },
    {
      "Sid" : "ListDomainBucketFromAthenaCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
      ],
      "Condition" : {
        "ArnEquals" : {
          "lambda:SourceFunctionArn" :
"arn:aws:lambda:*:*:function:athenafederatedcatalog_*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject",
```

```
        "s3:PutObjectRetention",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DomainBucketName" : ""
        }
      }
    },
    {
      "Sid" : "S3BucketAcl",
      "Effect" : "Allow",
      "Action" : "s3:GetBucketAcl",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BREvalS3Tag",
      "Effect" : "Allow",
      "Action" : "s3:PutObjectTagging",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
genAI/assets/evaluations/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "s3:RequestObjectTagKeys" : [
            "BasicValidationStatus",
            "ContainsReferenceResponseForAllPrompts"
```

```
          ]
        },
        "StringEquals" : {
          "s3:RequestObjectTag/BasicValidationStatus" : [
            "valid",
            "invalid"
          ],
          "s3:RequestObjectTag/ContainsReferenceResponseForAllPrompts" : [
            "true",
            "false"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DomainBucketName" : ""
        }
      }
    },
    {
      "Sid" : "DomainS3BucketKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DZDomainKMSKeyXAcctPerm",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
```

```
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/DomainKmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:aws:datazone:domainId" : "${aws:PrincipalTag/
AmazonDataZoneDomain}"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListLogGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueJobLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:PutLogEvents",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}/*"
      ]
    },
    {
      "Sid" : "ProjectLogGroup",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}",
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}:log-stream:*"
      ]
    },
    {
      "Sid" : "CloudWatchStopQuery",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataLakeAthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:UpdateNotebook",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
        "athena:DeleteNamedQuery",
        "athena:GetCalculationExecution",
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetNamedQuery",
```

```
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetSession",
        "athena:GetSessionStatus",
        "athena:GetWorkGroup",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "athena:ListQueryExecutions",
        "athena:ListTagsForResource",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AthenaDataCatalogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:datacatalog/AwsDataCatalog",
        "arn:aws:athena:*:*:datacatalog/awsdatacatalog"
```

```
      ]
    },
    {
      "Sid" : "AthenaListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListWorkGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneUserPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:CreateConnection",
        "datazone:DeleteConnection",
        "datazone:GetConnection",
        "datazone:GetDomain",
        "datazone:GetDomainExecutionRoleCredentials",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetProject",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListEnvironments",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListProjects",
        "datazone:UpdateConnection",
        "datazone:PostLineageEvent",
        "datazone:*Compute*"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/${aws:PrincipalTag/
AmazonDataZoneDomain}"
    },
    {
      "Sid" : "CodeConnectionsUser",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection",
        "codeconnections:UseConnection",
        "codestar-connections:GetConnection",
        "codestar-connections:UseConnection"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "GlueGetDefaultDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default"
      ]
    },
    {
      "Sid" : "AllowGlueGetDatabasesExceptDefault",
      "Effect" : "Allow",
      "Action" : "glue:GetDatabases",
      "NotResource" : "arn:aws:glue:*:*:database/default",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueListDatabasesOnNoDatabases",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases"
      ],
      "Resource" : "arn:aws:glue:*:*:catalog"
    },
    {
      "Sid" : "GlueFileUploadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetClassifier",
        "glue:GetClassifiers",
```

```
        "glue:UseGlueStudio"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueProjectConnectionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:RefreshOAuth2Tokens"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueGetConnectionOnlyOnCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:RefreshOAuth2Tokens"
      ],
      "Resource" : "arn:aws:glue:*:*:catalog"
    },
    {
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
```

```
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetDatabase",
        "glue:DeleteDatabase",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "S3TCatalogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:*ColumnStatistics*",
        "glue:*Database*",
```

```
        "glue:*Partition*",
        "glue:*Table*",
        "glue:GetCatalog*",
        "glue:GetUserDefinedFunction*"
      ],
      "Resource" : "arn:*:glue:*:*:catalog/s3tablescatalog"
    },
    {
      "Sid" : "GlueCrawler",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueGlobalTempDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueDefaultCatalogs",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
```

```
        }
      }
    },
    {
      "Sid" : "GlueNonDefaultCatalogs",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueCatalogDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "LFforDL",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess",
        "lakeformation:GetResourceLFTags"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "SetSourceIdentityForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
```

```
    {
      "Sid" : "TagSessionForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject",
            "AmazonDataZoneDomain"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "${aws:PrincipalTag/
AmazonDataZoneDomain}",
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SetContextForTIP",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : [
        "arn:aws:sts::*:self"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "sqlworkbench.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "StsContext",
      "Effect" : "Allow",
      "Action" : "sts:SetContext",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:ArnEquals" : {
```

```
          "sts:RequestContextProviders" : [
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
          ]
        },
        "Null" : {
          "sts:RequestContextProviders" : "false"
        }
      }
    },
    {
      "Sid" : "GlueConnectionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "UnrestrictedAccessGlueEntities",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListConnectionTypes",
        "glue:DescribeConnectionType"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueEntities",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListEntities",
        "glue:DescribeEntity",
        "glue:GetEntityRecords"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowPassRoleOnProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/${aws:PrincipalTag/RoleName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "airflow-serverless.amazonaws.com",
            "sagemaker.amazonaws.com",
            "glue.amazonaws.com",
            "airflow.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "scheduler.amazonaws.com",
            "access-grants.s3.amazonaws.com",
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SQLWorkBench",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:PutTab",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:ListTabs",
        "sqlworkbench:GetAutocompletion*",
        "sqlworkbench:PassAccountSettings",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:CreateConnection",
        "sqlworkbench:*QCustomContext",
        "sqlworkbench:GetQSql*",
        "sqlworkbench:GetSchemaInference"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "SQLWorkBenchActions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:AssociateNotebookWithTab",
      "Resource" : "arn:*:sqlworkbench:*:*:notebook/*"
    },
    {
      "Sid" : "SQLWorkBenchNotebookActions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateNotebook*",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook*",
        "sqlworkbench:DeleteNotebook*",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RSDataIAMSession",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
```

```
      "Sid" : "RedshiftDataActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ExistingRedshiftCompute",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift:DescribeTags",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "true"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "RedshiftWithoutResourceType",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RSWgTagged",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift:DescribeTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "RSExistCatalog",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowListSecrets",
      "Effect" : "Allow",
```

```
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeCredentials",
      "Effect" : "Allow",
      "Action" : [
        "emr-containers:*ManagedEndpoint*",
        "emr-containers:TagResource",
        "emr-containers:DescribeSecurityConfiguration",
        "emr-containers:DescribeVirtualCluster",
        "redshift-serverless:GetCredentials",
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "RSDataMWg",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:GetStagingBucketLocation",
        "redshift-serverless:GetManagedWorkgroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "redshift-data:glue-catalog-arn" : "arn:aws:glue:*:*:catalog/*"
        }
      }
    },
    {
      "Sid" : "RssCreds",
      "Effect" : "Allow",
```

```
      "Action" : [
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "redshift-data.amazonaws.com",
            "sqlworkbench.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowTagGetResources",
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowGetSecretForRedShift",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
```

```
      "Sid" : "CloudWatchMetricsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonQChatPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EMRClusterWithDataZoneTags",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetOnClusterAppUIPresignedURL",
        "elasticmapreduce:*Session*",
        "elasticmapreduce:AddTags"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EMRClusterInfoPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "elasticmapreduce:ListReleaseLabels",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:DescribePersistentAppUI",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EMRGetClusterSessionCreds",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:GetClusterSessionCredentials"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "elasticmapreduce:ExecutionRoleArn" : "arn:aws:iam::*:role/
${aws:PrincipalTag/RoleName}"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EmrContainersSSO",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "emr-containers.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "EMRPersistentAppUI",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:GetPersistentAppUIPresignedURL"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "elasticmapreduce:ExecutionRoleArn" : "arn:aws:iam::*:role/
${aws:PrincipalTag/RoleName}"
        }
      }
    },
    {
      "Sid" : "KmsWithEncrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "datazone.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "scheduler.*.amazonaws.com",
            "glue.*.amazonaws.com",
```

```
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EBDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "emr-serverless.*.amazonaws.com",
            "redshift.*.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "KmsManagement",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:RevokeGrant",
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "codecommit.*.amazonaws.com",
            "scheduler.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AwsOwnedKmsKeyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AwsOwnedKmsManagement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "EC2PermissionsForNotebookExecution",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "InvokeBRModel",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeModelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
```

```
        "ArnLike" : {
          "bedrock:InferenceProfileArn" : "arn:aws:bedrock:*:*:application-inference-
profile/*"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeBedrockModel",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BRInvokeAppProfile",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
```

```
      "Sid" : "AccessBedrockResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeAgent",
        "bedrock:Retrieve",
        "bedrock:ListIngestionJobs",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
        "bedrock:ApplyGuardrail",
        "bedrock:ListPrompts",
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
        "bedrock:GetEvaluationJob",
        "bedrock:CreateEvaluationJob",
        "bedrock:StopEvaluationJob",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:ListTagsForResource",
        "bedrock:CreateAgentAlias",
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentVersions",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:GetAgentAlias",
        "bedrock:UpdateAgentAlias"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockResourceAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ApplyGuardrail",
        "bedrock:BatchDeleteEvaluationJob",
```

```
        "bedrock:CreateAgentAlias",
        "bedrock:CreateBlueprint",
        "bedrock:CreateBlueprintVersion",
        "bedrock:CreateDataAutomationProject",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreatePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteBlueprint",
        "bedrock:DeleteDataAutomationProject",
        "bedrock:DeletePrompt",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentVersion",
        "bedrock:GetBlueprint",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataAutomationStatus",
        "bedrock:GetEvaluationJob",
        "bedrock:GetIngestionJob",
        "bedrock:GetPrompt",
        "bedrock:InvokeAgent",
        "bedrock:InvokeDataAutomationAsync",
        "bedrock:InvokeFlow",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentVersions",
        "bedrock:ListIngestionJobs",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:StopEvaluationJob",
        "bedrock:UpdateAgentAlias",
        "bedrock:UpdateBlueprint",
        "bedrock:UpdateDataAutomationProject",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentKnowledgeBases"
      ],
      "Resource" : "arn:aws:bedrock:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
```

```
      }
    },
    {
      "Sid" : "BREvalFM",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*"
      ]
    },
    {
      "Sid" : "BRCreateEval",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*::foundation-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeDataAutomationAsyncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeDataAutomationAsync"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:data-automation-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeBedrockInlineAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "bedrock:InlineAgentName" : "${datazone:userId}"
        },
        "StringNotEquals" : {
          "bedrock:InlineAgentName" : ""
        }
      }
    },
    {
      "Sid" : "BedrockInvokeInlineAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "bedrock:InlineAgentName" : "${datazone:userId}"
        },
        "StringNotEquals" : {
          "bedrock:InlineAgentName" : ""
        }
      }
    },
    {
      "Sid" : "BRRAG",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "ListBedrockEvaluationJobPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListEvaluationJobs",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockNoResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListEvaluationJobs",
        "bedrock:RetrieveAndGenerate",
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "PassRoleToBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*",
        "arn:aws:iam::*:role/AmazonBedrockServiceRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRoleToBedrock",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*",
        "arn:aws:iam::*:role/AmazonBedrockServiceRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "TagBedrockResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged",
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockTagResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "arn:aws:bedrock:*:*:*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonBedrockManaged",
```

```
            "AmazonDataZone*",
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KmsViaBedrockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
```

```
      "Condition" : {
        "ForAllValues:StringLike" : {
          "kms:EncryptionContextKeys" : [
            "aws:bedrock*:arn",
            "aws:bedrock:guardrail-id"
          ]
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretPermissionsForBedrockIDE",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerPermissionsForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SecretKmsPermissionsForBedrockIDE",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" :
 "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "BRKmsSM",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" :
 "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*"
        },
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InvokeFunctionForAmazonBedrockIDE",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "bedrock.amazonaws.com",
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "LambdaInvokeFunctionViaBedrock",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "bedrock.amazonaws.com",
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "DZEnvCfn",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CFNGetDataZoneEnvironmentStack",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncLF",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueGetUserDefinedFunc",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataConnectionAllProjectResources",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "glue:GetConnections"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "DataConnectionLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/athenafederatedcatalog*"
    },
    {
      "Sid" : "DataConnOpen",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "glue:ManagedConnector",
        "glue:TestConnection",
```

```
        "codeconnections:GetHost",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codestar-connections:GetHost",
        "codestar-connections:ListConnections",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataConnectionEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Vpc" : "${aws:PrincipalTag/vpcArn}"
        }
      }
    },
    {
      "Sid" : "DataConnectionDeleteENI",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:*/*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ec2:Vpc" : "${aws:PrincipalTag/vpcArn}"
        }
      }
    },
    {
      "Sid" : "DataConnectionDescribeENI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "PrivateECRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:CompleteLayerUpload",
        "ecr:DeleteRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:BatchDeleteImage",
        "ecr:ListTagsForResource",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:UploadLayerPart"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateECRRepositoryPermission",
      "Effect" : "Allow",
      "Action" : "ecr:CreateRepository",
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ECRTagResourcePermission",
      "Effect" : "Allow",
      "Action" : "ecr:TagResource",
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject",
            "ProjectUserTag*"
```

```
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ECRUntagResourcePermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:UntagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "LFResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:ListPermissions",
        "lakeformation:DescribeResource",
        "ram:GetResourceShareInvitations",
        "lakeformation:CreateDataCellsFilter",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:DeleteDataCellsFilter",
        "lakeformation:GetDataCellsFilter",
```

```
        "lakeformation:UpdateDataCellsFilter",
        "ram:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "XAcctLFCreate",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        }
      }
    },
    {
      "Sid" : "XAcctRAMGlue",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteResourcePolicy",
        "glue:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
```

```
        ]
      }
    }
  },
  {
    "Sid" : "XAcctRAMLF",
    "Effect" : "Allow",
    "Action" : [
      "ram:AssociateResourceShare",
      "ram:DisassociateResourceShare",
      "ram:DeleteResourceShare",
      "ram:ListResourceSharePermissions",
      "ram:UpdateResourceShare"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "lakeformation.amazonaws.com"
        ]
      },
      "StringLike" : {
        "ram:ResourceShareName" : [
          "LakeFormation*"
        ]
      }
    }
  },
  {
    "Sid" : "RAMGetResourceSharesViaLakeFormation",
    "Effect" : "Allow",
    "Action" : [
      "ram:GetResourceShares"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "lakeformation.amazonaws.com"
        ]
      }
    }
  },
  {
```

```
      "Sid" : "XAcctRAMInvite",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*",
            "DataZoneS3AG*"
          ]
        }
      }
    },
    {
      "Sid" : "XAcctRAMLFHybrid",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ram:PermissionArn" : "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EventBridgeScheduleActions",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:GetSchedule",
        "scheduler:UpdateSchedule",
        "scheduler:DeleteSchedule"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EventBridgeScheduleGroupActions",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:GetScheduleGroup"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "QSFolderDS",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSource",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:ListFolderMembers"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:folder/*",
        "arn:aws:quicksight:*:*:datasource/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ManageQuickSightOtherResources",
```

```
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSet",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeUser",
        "quicksight:DescribeGroup"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ]
    },
    {
      "Sid" : "ManagePassDataSourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:PassDataSource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ManageCreateDataSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSet",
        "quicksight:TagResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateFolderMembership",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateFolderMembership"
      ],
      "Resource" : "arn:aws:quicksight:*:*:folder/sagemaker-*-assets",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneAssetsFolder" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioQueryExecutionRolePolicy

Descrição: O Amazon SageMaker Studio usa essa política ao executar execuções de consultas em conexões federadas.

`SageMakerStudioQueryExecutionRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioQueryExecutionRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 31 de janeiro de 2025, 19:52 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioQueryExecutionRolePolicy`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueGetConnectionOnCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueGetConnectionsForProject",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : "arn:aws:glue:*:*:connection/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "S3GetObjectForAthenaSpillBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/dzd*/*/dev/sys/athena/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        }
      }
    },
    {
      "Sid" : "S3ListBucketOwnershipCheckForAthenaSpillBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeFunctionPermissionsForAthenaCatalogLambda",
      "Effect" : "Allow",
```

```
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceTag/federated_athena_datacatalog" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioUserIAMConsolePolicy

Descrição: Fornece privilégios de configuração individuais para o Amazon SageMaker Unified Studio por meio do SDK Console de gerenciamento da AWS e. Permite o lançamento do SageMaker Unified Studio Portal.

`SageMakerStudioUserIAMConsolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioUserIAMConsolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 18 de agosto de 2025, 22:49 UTC
- Horário editado: 31 de março de 2026, 21:12 UTC

- ARN: `arn:aws:iam::aws:policy/SageMakerStudioUserIAMConsolePolicy`

Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:ListDomains",
        "datazone:GetDomain",
        "datazone:GetUserProfile",
        "datazone:ListProjects",
        "datazone:ListProjectProfiles",
        "datazone:CreateProject",
        "datazone:GetProject",
        "datazone:DeleteProject",
        "datazone:GetIamPortalLoginUrl",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironments",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetGroupProfile",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "datazone:ListProjectMemberships",
        "datazone:GetConnection",
        "datazone:ListConnections"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioUserIAMDefaultExecutionPolicy

Descrição: Política de execução para usar funções do IAM com o SageMaker Unified Studio. Permite que os usuários acessem recursos na conta local (excluindo o acesso aos recursos de dados) para IAM-based uso do SageMaker Unified Studio.

`SageMakerStudioUserIAMDefaultExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioUserIAMDefaultExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 18 de agosto de 2025, 17:19 UTC
- Horário editado: 13 de agosto de 2026, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy`

Versão da política

Versão da política: v29 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:BatchUpdateNotifications",
```

```
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset*",
        "datazone:CreateConnection",
        "datazone:CreateEnvironment",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset*",
        "datazone:DeleteConnection",
        "datazone:DeleteEnvironment",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:Get*",
        "datazone:List*",
        "datazone:PostLineageEvent",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateEnvironment",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionRequest",
        "datazone:*Notebook*",
        "datazone:CreateCell",
        "datazone:UpdateCell",
        "datazone:DeleteCell",
        "datazone:BatchGetCell",
        "datazone:CreateCellRun",
        "datazone:UpdateCellRun",
        "datazone:DeleteCellRun",
        "datazone:BatchGetCellRun",
        "datazone:PutCellRunResult",
```

```
        "datazone:StartConversation",
        "datazone:GenerateCode",
        "datazone:SendMessage",
        "datazone:CancelMessage",
        "datazone:QueryGraph",
        "datazone:StartCompute",
        "datazone:StopCompute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
```

```
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless"
      ]
    },
    {
      "Sid" : "TagSession",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "Q",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "q:Get*",
        "q:List*",
        "q:PassRequest",
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "SageMakerUserTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile",
        "sagemaker:UpdateUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerPrivateSpace",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
```

```
        "sagemaker:CreateSpace",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:app/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "CanvasUserProfileApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp",
        "sagemaker:CreateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/Canvas/*",
        "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "AllowStartSessionForSpaceRemoteConnection",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StartSession"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Batch*",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sagemaker:Search",
        "sagemaker:*Endpoint*",
        "sagemaker:*Model*",
        "sagemaker:*Context*",
        "sagemaker:*Artifact*",
        "sagemaker:*Action*",
        "sagemaker:*Association*",
        "sagemaker:QueryLineage",
        "sagemaker:*InferenceComponent*",
        "sagemaker:*Job*",
        "sagemaker:*MlflowApp*",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*",
        "sagemaker:*Feature*",
        "sagemaker:*Record"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerTagPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*",
            "sagemaker*",
            "sm-jumpstart*",
            "endpoint-has-jumpstart-model",
            "aws-jumpstart*",
            "Source",
            "CanvasModelName",
            "Canvas",
            "SageMaker",
            "ProjectS3Path",
            "Owner"
          ]
        },
        "ForAllValues:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "sagemaker:shared-with:*"
          ]
        }
      }
    },
    {
      "Sid" : "LogsAndMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:GetMetricData",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:Describe*",
        "logs:Get*",
        "logs:PutLogEvents",
```

```
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Glue",
      "Effect" : "Allow",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:CreateCatalog",
        "glue:Describe*",
        "glue:Get*",
        "glue:List*",
        "glue:NotifyEvent",
        "glue:RunStatement",
        "glue:StartCompletion",
        "glue:StopSession",
        "glue:UseGlueStudio",
        "glue:*Resource",
        "glue:*Job*",
        "glue:TestConnection",
        "glue:*DataQuality*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyForeignSessionAccess",
      "Effect" : "Deny",
      "Action" : [
        "athena:GetResourceDashboard",
        "athena:GetSession",
        "athena:GetSessionEndpoint",
        "athena:GetSessionStatus",
        "athena:StartSession",
        "athena:TerminateSession",
        "emr-serverless:*Session*",
        "emr-serverless:*Dashboard*",
        "emr-containers:*ManagedEndpoint*",
        "elasticmapreduce:*Session*",
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
```

```
        "glue:GetDashboardUrl",
        "glue:GetSession",
        "glue:GetSessionEndpoint",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource",
        "emr-serverless:*Resource",
        "emr-containers:*Resource",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
```

```
        }
      }
    },
    {
      "Sid" : "GlueDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "GlueLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListPermissions",
        "lakeformation:RevokePermissions"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "SQLWorkBench",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftData",
      "Effect" : "Allow",
      "Action" : "redshift-data:*",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedShiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:Describe*",
        "redshift-data:ExecuteStatement",
        "redshift-data:List*",
        "redshift-serverless:GetManagedWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Bedrock",
      "Effect" : "Allow",
      "Action" : "bedrock:*",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/${aws:PrincipalTag/
AmazonDataZonePassedRolePath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "bedrock.amazonaws.com",
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "sagemaker.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "redshift.amazonaws.com",
            "airflow-serverless.amazonaws.com",
            "events.amazonaws.com",
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AirflowServerless",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:List*",
        "airflow-serverless:Get*",
        "airflow-serverless:CreateWorkflow",
        "airflow-serverless:UpdateWorkflow",
        "airflow-serverless:DeleteWorkflow",
        "airflow-serverless:StartWorkflowRun",
        "airflow-serverless:StopWorkflowRun",
        "airflow-serverless:TagResource",
        "airflow-serverless:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowMWAA",
```

```
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3List",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Scheduler",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:DeleteSchedule",
        "scheduler:Get*",
        "scheduler:List*",
        "scheduler:UpdateSchedule"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Athena",
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGet*",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:Get*",
        "athena:ImportNotebook",
        "athena:List*",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TagResource",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateSecret",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${datazone:projectId}"
        }
      }
    },
    {
      "Sid" : "SharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "GenerateRecommendations",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ecr",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsUser",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection",
        "codeconnections:UseConnection",
        "codestar-connections:GetConnection",
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "CodeConnectionsUserList",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetHost",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codestar-connections:GetHost",
        "codestar-connections:ListConnections",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
```

```
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "AccessProjectS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject*",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject*",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/AmazonDataZoneProjectBucket}/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProjectBucket" : ""
        }
      }
    },
    {
```

```
      "Sid" : "EMR",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:Get*",
        "emr-serverless:List*",
        "emr-serverless:Start*",
        "emr-serverless:Access*Endpoints",
        "emr-serverless:Terminate*",
        "emr-serverless:*Resource",
        "emr-containers:*ManagedEndpoint*",
        "emr-containers:*SecurityConfiguration*",
        "emr-containers:*VirtualCluster*",
        "emr-containers:*Resource",
        "elasticmapreduce:*PersistentAppUI*",
        "elasticmapreduce:Start*",
        "elasticmapreduce:Get*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elasticmapreduce:Terminate*",
        "elasticmapreduce:*Tag*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CanvasGeneralPermissions",
      "Effect" : "Allow",
      "Action" : [
        "comprehend:BatchDetect*",
        "comprehend:Detect*",
        "textract:Analyze*",
        "textract:Start*",
        "textract:Get*",
        "rekognition:Detect*",
        "sagemaker-data-science-assistant:*",
        "rds:DescribeDBInstances",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalingActivities",
        "quicksight:ListNamespaces",
        "events:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CanvasRedshiftAccess",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "CanvasEventBridgePutOperation",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "CanvasEventBridgeOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "CanvasEventBridgeTagBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SageMakerStudioUserIAMPermissiveExecutionPolicy

Descrição: Política de execução para usar funções do IAM com o SageMaker Unified Studio. Permite que os usuários acessem recursos em sua conta (incluindo amplo acesso a todas as APIs em serviços de dados como S3, Glue, CloudWatch Logs e outros) para IAM-based uso do SageMaker Unified Studio.

`SageMakerStudioUserIAMPermissiveExecutionPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SageMakerStudioUserIAMPermissiveExecutionPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 18 de agosto de 2025, 17:19 UTC
- Horário editado: 13 de agosto de 2026, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy`

Versão da política

Versão da política: v24 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "glue:*",
        "logs:*",
        "redshift-data:*",
        "redshift-serverless:*",
        "redshift:*",
        "s3:*",
        "s3tables:*",
        "comprehend:*",
        "textract:*",
        "rekognition:*",
        "sagemaker-data-science-assistant:*",
        "rds:*",
        "quicksight:*",
        "events:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeAccess",
      "Effect" : "Allow",
      "Action" : [
        "athena:*",
        "bedrock:*",
        "codewhisperer:*",
        "sagemaker-unified-studio-mcp:*",
```

```
        "elasticmapreduce:*",
        "emr-containers:*",
        "q:*",
        "sagemaker:*",
        "sagemaker-mlflow:*",
        "scheduler:*",
        "sqlworkbench:*",
        "emr-serverless:*",
        "airflow-serverless:*",
        "airflow:*",
        "application-autoscaling:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyForeignSessionAccess",
      "Effect" : "Deny",
      "Action" : [
        "athena:GetResourceDashboard",
        "athena:GetSession",
        "athena:GetSessionEndpoint",
        "athena:GetSessionStatus",
        "athena:StartSession",
        "athena:TerminateSession",
        "emr-serverless:*Session*",
        "emr-serverless:*Dashboard*",
        "emr-containers:*ManagedEndpoint*",
        "elasticmapreduce:*Session*",
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetDashboardUrl",
        "glue:GetSession",
        "glue:GetSessionEndpoint",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
```

```
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource",
        "emr-serverless:*Resource",
        "emr-containers:*Resource",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*",
        "arn:aws:emr-serverless:*:*:/applications/*/sessions/*",
        "arn:aws:emr-containers:*:*:/virtualclusters/*/endpoints/*",
        "arn:aws:elasticmapreduce:*:*:cluster/*/session/*",
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:BatchUpdateNotifications",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset*",
```

```
        "datazone:CreateConnection",
        "datazone:CreateEnvironment",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset*",
        "datazone:DeleteConnection",
        "datazone:DeleteEnvironment",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:Get*",
        "datazone:List*",
        "datazone:PostLineageEvent",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateEnvironment",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionRequest",
        "datazone:*Notebook*",
        "datazone:CreateCell",
        "datazone:UpdateCell",
        "datazone:DeleteCell",
        "datazone:BatchGetCell",
        "datazone:CreateCellRun",
        "datazone:UpdateCellRun",
        "datazone:DeleteCellRun",
        "datazone:BatchGetCellRun",
        "datazone:PutCellRunResult",
        "datazone:StartConversation",
        "datazone:GenerateCode",
        "datazone:SendMessage",
```

```
        "datazone:CancelMessage",
        "datazone:QueryGraph",
        "datazone:StartCompute",
        "datazone:StopCompute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
```

```
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless"
      ]
    },
    {
      "Sid" : "TagSession",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "glue.amazonaws.com",
            "bedrock.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "scheduler.amazonaws.com",
```

```
            "emr-serverless.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "airflow-serverless.amazonaws.com",
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListPermissions",
        "lakeformation:RevokePermissions"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets",
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${datazone:projectId}"
        }
      }
    },
    {
      "Sid" : "SharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
```

```
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsUser",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection",
        "codeconnections:UseConnection",
        "codestar-connections:GetConnection",
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "CodeConnectionsUserList",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetHost",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
```

```
        "codestar-connections:GetHost",
        "codestar-connections:ListConnections",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
```

```
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
```

```
          "kms:EncryptionContextKeys" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SecretsManagerReadWrite

Descrição: Fornece read/write acesso ao AWS Secrets Manager por meio do Console de gerenciamento da AWS. Observação: isso exclui as ações do IAM, portanto, combine com IAMFullAccess se a configuração de rotação for necessária.

`SecretsManagerReadWrite` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SecretsManagerReadWrite` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 04 de abril de 2018, 18:05 UTC
- Horário editado: 25 de agosto de 2026, 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/SecretsManagerReadWrite`

Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:*",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResource",
```

```
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "lambda:ListFunctions",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:SecretsManager*"
    },
    {
      "Sid" : "SARPermissions",
      "Effect" : "Allow",
      "Action" : [
        "serverlessrepo:CreateCloudFormationChangeSet",
        "serverlessrepo:GetApplication"
      ],
      "Resource" : "arn:aws:serverlessrepo:*:*:applications/SecretsManager*"
    },
    {
      "Sid" : "S3Permissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::awsserverlessrepo-changesets*",
        "arn:aws:s3:::secrets-manager-rotation-apps-*/*"
      ]
    },
    {
      "Sid" : "CloudFormationTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudformation:CreateAction" : [
            "CreateChangeSet",
            "ExecuteChangeSet"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SecurityAgentWebAppAPIPolicy

Descrição: Fornece permissões para usuários autenticados acessarem o aplicativo Web do Security Agent para configurar e executar testes automatizados de penetração de segurança. Essa política

permite que os usuários gerenciem pentests, visualizem descobertas, monitorem a execução de testes e interajam com AWS os recursos necessários para operações de teste de segurança.

`SecurityAgentWebAppAPIPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SecurityAgentWebAppAPIPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 02 de dezembro de 2025, 15:04 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SecurityAgentWebAppAPIPolicy`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:ListAgentInstances",
        "securityagent:ListControls"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "AgentInstanceAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:AddArtifact",
        "securityagent:BatchDeletePentests",
        "securityagent:BatchGetAgentInstances",
        "securityagent:BatchGetArtifactMetadata",
        "securityagent:BatchGetFindings",
        "securityagent:BatchGetPentestJobs",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetSecurityTestContentMetadata",
        "securityagent:BatchGetTasks",
        "securityagent:CreateDocumentReview",
        "securityagent:CreatePentest",
        "securityagent:DeleteArtifact",
        "securityagent:DeleteDocumentReview",
        "securityagent:GetArtifact",
        "securityagent:GetCodeReviewTask",
        "securityagent:GetDocReviewTask",
        "securityagent:GetDocumentReview",
        "securityagent:GetDocumentReviewArtifact",
        "securityagent:ListArtifacts",
        "securityagent:ListControls",
        "securityagent:ListDiscoveredEndpoints",
        "securityagent:ListDocumentReviewComments",
        "securityagent:ListDocumentReviews",
        "securityagent:ListFindings",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentestJobsForPentest",
        "securityagent:ListPentests",
        "securityagent:ListTasks",
        "securityagent:StartCodeRemediation",
        "securityagent:StartPentestExecution",
        "securityagent:StopPentestExecution",
        "securityagent:UpdateFinding",
        "securityagent:UpdatePentest"
      ],
      "Resource" : "arn:aws:securityagent:*:*:agent-instance*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SecurityAgentWebAppPolicy

Descrição: Fornece permissões para usuários autenticados acessarem o aplicativo Web do Security Agent para configurar e executar testes automatizados de penetração de segurança. Essa política permite que os usuários gerenciem pentests, visualizem descobertas, monitorem a execução de testes e interajam com AWS os recursos necessários para operações de teste de segurança.

`SecurityAgentWebAppPolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SecurityAgentWebAppPolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 05 de fevereiro de 2026, 20:19 UTC
- Horário editado: 12 de fevereiro de 2026, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAgentWebAppPolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:ListAgentSpaces",
        "securityagent:ListSecurityRequirements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentSpaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:AddArtifact",
        "securityagent:BatchDeletePentests",
        "securityagent:BatchGetAgentSpaces",
        "securityagent:BatchGetArtifactMetadata",
        "securityagent:BatchGetFindings",
        "securityagent:BatchGetPentestJobs",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetPentestJobContentMetadata",
        "securityagent:BatchGetPentestJobTasks",
        "securityagent:CreateDesignReview",
        "securityagent:CreatePentest",
        "securityagent:DeleteArtifact",
        "securityagent:GetArtifact",
        "securityagent:DeleteDesignReview",
        "securityagent:GetDesignReview",
        "securityagent:GetDesignReviewArtifact",
```

```
        "securityagent:ListArtifacts",
        "securityagent:ListSecurityRequirements",
        "securityagent:ListDiscoveredEndpoints",
        "securityagent:ListDesignReviewComments",
        "securityagent:ListDesignReviews",
        "securityagent:ListFindings",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentestJobsForPentest",
        "securityagent:ListPentests",
        "securityagent:ListPentestJobTasks",
        "securityagent:StartCodeRemediation",
        "securityagent:StartPentestJob",
        "securityagent:StopPentestJob",
        "securityagent:UpdateFinding",
        "securityagent:UpdatePentest"
      ],
      "Resource" : "arn:aws:securityagent:*:*:agent-space*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SecurityAudit

Descrição: o modelo de auditoria de segurança concede acesso para leitura de metadados de configuração de segurança. É útil para software que audita a configuração de uma Conta da AWS.

`SecurityAudit` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SecurityAudit` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 30 de setembro de 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAudit`

Versão da política

Versão da política: v94 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseSecurityAuditStatement",
      "Effect" : "Allow",
      "Action" : [
        "a4b:ListSkills",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListTagsForResource",
        "account:GetAccountInformation",
        "account:GetAlternateContact",
```

```
        "account:GetPrimaryEmail",
        "account:GetRegionOptStatus",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetPolicy",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags",
        "acm:Describe*",
        "acm:List*",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "amplify:GetWebACLForResource",
        "amplify:ListDomainAssociations",
        "amplify:ListResourcesForWebACL",
        "apigateway:GetPortal",
        "apigateway:GetPortalProduct",
        "apigateway:GetPortalProductSharingPolicy",
        "apigateway:GetRoutingRule",
        "apigateway:ListPortalProducts",
        "apigateway:ListPortals",
        "apigateway:ListProductPages",
        "apigateway:ListProductRestEndpointPages",
        "apigateway:ListRoutingRules",
        "appconfig:GetAccountSettings",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExperimentDefinition",
        "appconfig:GetExtension",
        "appconfig:GetExtensionAssociation",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListDeployments",
        "appconfig:ListEnvironments",
        "appconfig:ListExperimentDefinitions",
        "appconfig:ListExperimentRuns",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:ListFlows",
```

```
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appsync:GetApi",
        "appsync:GetApiCache",
        "appsync:GetChannelNamespace",
        "appsync:GetGraphqlApi",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResourcePolicy",
        "appsync:GetSourceApiAssociation",
        "appsync:List*",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:ListAssessmentControlInsightsByControlDomain",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentFrameworkShareRequests",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
        "auditmanager:ListControlDomainInsights",
        "auditmanager:ListControlDomainInsightsByAssessment",
        "auditmanager:ListControlInsightsByControlDomain",
        "auditmanager:ListControls",
        "auditmanager:ListNotifications",
        "auditmanager:ListTagsForResource",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling:Describe*",
        "backup:DescribeBackupVault",
        "backup:DescribeGlobalSettings",
```

```
        "backup:DescribeRegionSettings",
        "backup:GetBackupPlan",
        "backup:GetBackupPlanFromJSON",
        "backup:GetBackupPlanFromTemplate",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListProtectedResources",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobDefinitions",
        "bedrock:CheckIngestedDocumentAcl",
        "bedrock:GetAccountDataRetention",
        "bedrock:GetAdvancedPromptOptimizationJob",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:GetAsyncInvoke",
        "bedrock:GetAutomatedReasoningPolicy",
        "bedrock:GetAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:GetAutomatedReasoningPolicyNextScenario",
        "bedrock:GetBlueprint",
        "bedrock:GetBlueprintOptimizationStatus",
        "bedrock:GetBlueprintRecommendation",
        "bedrock:GetCustomModel",
        "bedrock:GetCustomModelDeployment",
        "bedrock:GetDataAutomationLibrary",
        "bedrock:GetDataAutomationLibraryIngestionJob",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataAutomationStatus",
        "bedrock:GetDataSource",
        "bedrock:GetEvaluationJob",
        "bedrock:GetExecutionFlowSnapshot",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowExecution",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
```

```
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetGuardrail",
        "bedrock:GetImportedModel",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestedDocumentAcl",
        "bedrock:GetIngestionJob",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetKnowledgeBaseDocuments",
        "bedrock:GetMarketplaceModelEndpoint",
        "bedrock:GetModelCopyJob",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelImportJob",
        "bedrock:GetModelInvocationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPromptRouter",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:GetResourcePolicy",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAgentVersions",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListFlowVersions",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListImportedModels",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListIngestionJobs",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListMarketplaceModelEndpoints",
        "bedrock:ListModelCopyJobs",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListModelImportJobs",
        "bedrock:ListModelInvocationJobs",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListProvisionedModelThroughputs",
        "bedrock:ListTagsForResource",
        "bedrock-agentcore:GetABTest",
```

```
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBatchEvaluation",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetBrowserProfile",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetConfigurationBundle",
        "bedrock-agentcore:GetConfigurationBundleVersion",
        "bedrock-agentcore:GetEvaluator",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetHarness",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetOnlineEvaluationConfig",
        "bedrock-agentcore:GetPaymentConnector",
        "bedrock-agentcore:GetPaymentCredentialProvider",
        "bedrock-agentcore:GetPaymentInstrument",
        "bedrock-agentcore:GetPaymentManager",
        "bedrock-agentcore:GetPaymentSession",
        "bedrock-agentcore:GetPolicy",
        "bedrock-agentcore:GetPolicyEngine",
        "bedrock-agentcore:GetPolicyGeneration",
        "bedrock-agentcore:GetRecommendation",
        "bedrock-agentcore:GetRegistry",
        "bedrock-agentcore:GetRegistryRecord",
        "bedrock-agentcore:GetResourcePolicy",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:ListABTests",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimeVersions",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBatchEvaluations",
        "bedrock-agentcore:ListBrowserProfiles",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListConfigurationBundleVersions",
        "bedrock-agentcore:ListConfigurationBundles",
        "bedrock-agentcore:ListEvaluators",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListHarnesses",
```

```
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListOnlineEvaluationConfigs",
        "bedrock-agentcore:ListPaymentConnectors",
        "bedrock-agentcore:ListPaymentCredentialProviders",
        "bedrock-agentcore:ListPaymentInstruments",
        "bedrock-agentcore:ListPaymentManagers",
        "bedrock-agentcore:ListPaymentSessions",
        "bedrock-agentcore:ListPolicies",
        "bedrock-agentcore:ListPolicyEngines",
        "bedrock-agentcore:ListPolicyGenerationAssets",
        "bedrock-agentcore:ListPolicyGenerations",
        "bedrock-agentcore:ListRecommendations",
        "bedrock-agentcore:ListRegistries",
        "bedrock-agentcore:ListRegistryRecords",
        "bedrock-agentcore:ListTagsForResource",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "chime:List*",
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaborationConfiguredAudienceModelAssociation",
        "cleanrooms:GetCollaborationIdNamespaceAssociation",
        "cleanrooms:GetCollaborationPrivacyBudgetTemplate",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetConfiguredTableAssociationAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborationIdNamespaceAssociations",
```

```
        "cleanrooms:ListCollaborationPrivacyBudgets",
        "cleanrooms:ListCollaborationPrivacyBudgetTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredAudienceModelAssociations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgets",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:PreviewPrivacyImpact",
        "cloud9:Describe*",
        "cloud9:ListEnvironments",
        "clouddirectory:ListDirectories",
        "cloudformation:DescribeStack*",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudformation:ListStack*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:DescribeDomainEndpointOptions",
        "cloudsearch:DescribeDomains",
        "cloudsearch:DescribeServiceAccessPolicies",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetrics",
```

```
        "cloudwatch:ListTagsForResource",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListRepositories",
        "codebuild:BatchGetProjects",
        "codebuild:GetResourcePolicy",
        "codebuild:ListProjects",
        "codebuild:ListSourceCredentials",
        "codecommit:BatchGetRepositories",
        "codecommit:GetBranch",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:List*",
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:GetJobDetails",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "codestar:Describe*",
        "codestar:List*",
        "cognito-identity:Describe*",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentities",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:Describe*",
        "cognito-idp:ListDevices",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserImportJobs",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListUsersInGroup",
        "cognito-sync:Describe*",
```

```
        "cognito-sync:List*",
        "comprehend:Describe*",
        "comprehend:List*",
        "comprehendmedical:ListICD10CMInferenceJobs",
        "comprehendmedical:ListPHIDetectionJobs",
        "comprehendmedical:ListRxNormInferenceJobs",
        "comprehendmedical:ListSNOMEDCTInferenceJobs",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:ListApprovedOrigins",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListLambdaFunctions",
        "connect:ListLexBots",
        "connect:ListSecurityKeys",
        "databrew:DescribeDataset",
        "databrew:DescribeProject",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "dataexchange:ListDataSets",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:EvaluateExpression",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "datapipeline:ValidatePipelineDefinition",
        "datasync:Describe*",
        "datasync:List*",
        "dax:Describe*",
        "dax:ListTags",
        "deepracer:ListModels",
        "detective:GetGraphIngestState",
        "detective:ListGraphs",
        "detective:ListMembers",
        "devicefarm:ListProjects",
```

```
        "directconnect:Describe*",
        "discovery:DescribeAgents",
        "discovery:DescribeConfigurations",
        "discovery:DescribeContinuousExports",
        "discovery:DescribeExportConfigurations",
        "discovery:DescribeExportTasks",
        "discovery:DescribeImportTasks",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "dlm:ListTagsForResource",
        "dms:Describe*",
        "dms:ListTagsForResource",
        "docdb-elastic:ListClusters",
        "ds:DescribeDirectories",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeEndpoints",
        "dynamodb:DescribeExport",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeImport",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetAbacStatus",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListBackups",
        "dynamodb:ListContributorInsights",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListImports",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:GetActiveVpnTunnelStatus",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
```

```
        "ec2:GetAssociatedIpv6PoolCidrs",
        "ec2:GetCapacityManagerAttributes",
        "ec2:GetCapacityManagerMetricDimensions",
        "ec2:GetCapacityManagerMonitoredTagKeys",
        "ec2:GetCapacityReservationUsage",
        "ec2:GetCoipPoolUsage",
        "ec2:GetDeclarativePoliciesReportSummary",
        "ec2:GetDefaultCreditSpecification",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEnabledIpamPolicy",
        "ec2:GetFlowLogsIntegrationTemplate",
        "ec2:GetGroupsForCapacityReservation",
        "ec2:GetHostReservationPurchasePreview",
        "ec2:GetImageAncestry",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetInstanceMetadataDefaults",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamAddressHistory",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "ec2:GetIpamDiscoveredRoutes",
        "ec2:GetIpamInternetRegistryAssociationAsns",
        "ec2:GetIpamInternetRegistryAssociationCidrs",
        "ec2:GetIpamPolicyAllocationRules",
        "ec2:GetIpamPolicyOrganizationTargets",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetIpamPrefixListResolverRules",
        "ec2:GetIpamPrefixListResolverVersions",
        "ec2:GetIpamResourceCidrs",
        "ec2:GetIpamRouteOriginAuthorizations",
        "ec2:GetIpamRouteProtectionFindings",
        "ec2:GetIpamRoutingPolicyRegistrations",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedResourceVisibility",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetReservedInstancesExchangeQuote",
        "ec2:GetResourcePolicy",
        "ec2:GetRouteServerAssociations",
        "ec2:GetRouteServerPropagations",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:GetSerialConsoleAccessStatus",
```

```
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetSpotPlacementScores",
        "ec2:GetSubnetCidrReservations",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayMeteringPolicyEntries",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:GetTransitGatewayPolicyTableEntries",
        "ec2:GetTransitGatewayPrefixListReferences",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessEndpointTargets",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:GetVpcResourcesBlockingEncryptionEnforcement",
        "ec2:GetVpnConnectionDeviceTypes",
        "ec2:GetVpnTunnelReplacementStatus",
        "ec2:ListImagesInRecycleBin",
        "ec2:ListSnapshotsInRecycleBin",
        "ec2:ListVolumesInRecycleBin",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImages",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecs:Describe*",
```

```
        "ecs:List*",
        "eks:DescribeAccessEntry",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodeGroup",
        "eks:ListAccessEntries",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodeGroups",
        "eks:ListTagsForResource",
        "eks:ListUpdates",
        "elasticache:Describe*",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:ListTagsForResource",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elastictranscoder:ListPipelines",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdNamespace",
```

```
        "es:Describe*",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListElasticsearchInstanceTypeDetails",
        "es:ListElasticsearchVersions",
        "es:ListTags",
        "events:Describe*",
        "events:List*",
        "events:TestEventPattern",
        "finspace:ListEnvironments",
        "finspace:ListKxEnvironments",
        "firehose:Describe*",
        "firehose:List*",
        "fms:ListComplianceStatus",
        "fms:ListPolicies",
        "forecast:ListDatasets",
        "frauddetector:GetDetectors",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "geo:ListMaps",
        "glacier:DescribeJob",
        "glacier:DescribeVault",
        "glacier:GetDataRetrievalPolicy",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultLock",
        "glacier:GetVaultNotifications",
        "glacier:ListJobs",
        "glacier:ListTagsForVault",
        "glacier:ListVaults",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:GetCrawlers",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoints",
        "glue:GetJobBookmark",
        "glue:GetJobRuns",
        "glue:GetJobs",
        "glue:GetResourcePolicies",
        "glue:GetResourcePolicy",
        "glue:GetSchema",
        "glue:GetSecurityConfiguration",
```

```
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:GetTags",
        "glue:ListJobs",
        "glue:ListSchemaVersions",
        "glue:ListSchemas",
        "glue:ListSessions",
        "grafana:ListWorkspaces",
        "greengrass:List*",
        "guardduty:DescribeMalwareScans",
        "guardduty:DescribeOrganizationConfiguration",
        "guardduty:DescribePublishingDestination",
        "guardduty:Get*",
        "guardduty:List*",
        "health:DescribeAffectedAccountsForOrganization",
        "health:DescribeAffectedEntities",
        "health:DescribeAffectedEntitiesForOrganization",
        "health:DescribeEntityAggregates",
        "health:DescribeEventAggregates",
        "health:DescribeEventDetails",
        "health:DescribeEventDetailsForOrganization",
        "health:DescribeEvents",
        "health:DescribeEventsForOrganization",
        "health:DescribeEventTypes",
        "health:DescribeHealthServiceStatusForOrganization",
        "healthlake:ListFHIRDatastores",
        "honeycode:ListTables",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy",
        "identitystore:DescribeGroupMembership",
        "identitystore:GetGroupId",
        "identitystore:GetGroupMembershipId",
        "identitystore:GetUserId",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
```

```
        "identitystore:ListUsers",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "iot:Describe*",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:List*",
        "iotanalytics:ListChannels",
        "iotevents:ListInputs",
        "iotfleetwise:ListModelManifests",
        "iotsitewise:DescribeGatewayCapabilityConfiguration",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListGateways",
        "iottwinmaker:ListWorkspaces",
        "kafka-cluster:Describe*",
        "kafka:Describe*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:DescribeIndex",
        "kendra:ListDataSources",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeLimits",
```

```
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListShards",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeEdgeConfiguration",
        "kinesisvideo:DescribeMappedResourceConfiguration",
        "kinesisvideo:DescribeMediaStorageConfiguration",
        "kinesisvideo:DescribeNotificationConfiguration",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lambda:GetAccountSettings",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetResourcePolicy",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
        "lex:DescribeBot",
        "lex:DescribeResourcePolicy",
        "lex:ListBots",
        "license-manager:List*",
        "lightsail:GetBuckets",
        "lightsail:GetContainerServices",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetInstancePortStates",
        "lightsail:GetInstances",
```

```
        "lightsail:GetLoadBalancers",
        "lightsail:GetStaticIps",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "lookoutequipment:ListDatasets",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutvision:ListProjects",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:DescribeMLModels",
        "macie2:ListFindings",
        "managedblockchain:ListNetworks",
        "mechanicalturk:ListHITs",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:ListChannels",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:DescribeOriginEndpoint",
        "mediapackage:ListOriginEndpoints",
        "mediastore:DescribeContainer",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:GetLifecyclePolicy",
        "mediastore:ListContainers",
        "mediastore:ListTagsForResource",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeUsers",
        "mq:DescribeBroker",
        "mq:DescribeBrokerEngineTypes",
        "mq:DescribeBrokerInstanceOptions",
        "mq:DescribeConfiguration",
        "mq:DescribeConfigurationRevision",
        "mq:DescribeUser",
        "mq:ListBrokers",
        "mq:ListConfigurationRevisions",
        "mq:ListConfigurations",
```

```
        "mq:ListTags",
        "mq:ListUsers",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "networkmanager:DescribeGlobalNetworks",
        "nimble:ListStudios",
        "opsworks-cm:DescribeServers",
        "opsworks:DescribeStacks",
        "organizations:Describe*",
        "organizations:List*",
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "personalize:DescribeDatasetGroup",
        "personalize:ListDatasetGroups",
        "private-networks:ListNetworks",
        "profile:GetDomain",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "qapps:GetQApp",
        "qapps:ListQApps",
        "qapps:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetPolicy",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:ListApplications",
        "qbusiness:ListDataSources",
        "qbusiness:ListDataSourceSyncJobs",
        "qbusiness:ListDocuments",
        "qbusiness:ListGroups",
```

```
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListSubscriptions",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "quicksight:Describe*",
        "quicksight:List*",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:List*",
        "rds:Describe*",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetResourcePolicy",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:Describe*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resource-groups:ListGroupResources",
        "robomaker:Describe*",
        "robomaker:List*",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53:Get*",
        "route53:List*",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:ListDomains",
```

```
        "route53domains:ListOperations",
        "route53domains:ListTagsForDomain",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListSharedEndpoints",
        "s3:DescribeJob",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrantsInstanceResourcePolicy",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucket*",
        "s3:GetEncryptionConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListCallerAccessGrants",
        "s3:ListJobs",
        "s3:ListMultiRegionAccessPoints",
```

```
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:ListAllMyDirectoryBuckets",
        "s3files:GetAccessPoint",
        "s3files:GetFileSystem",
        "s3files:GetFileSystemPolicy",
        "s3files:GetMountTarget",
        "s3files:GetSynchronizationConfiguration",
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems",
        "s3files:ListMountTargets",
        "s3files:ListTagsForResource",
        "s3tables:GetNamespace",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableMaintenanceConfiguration",
        "s3tables:GetTablePolicy",
        "s3tables:ListNamespaces",
        "s3tables:ListTableBuckets",
        "s3tables:ListTables",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:GetVectors",
        "s3vectors:ListIndexes",
        "s3vectors:ListVectorBuckets",
        "s3vectors:ListVectors",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "sdb:DomainMetadata",
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
```

```
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetConfigurationPolicyAssociations",
        "securityhub:BatchGetControlEvaluations",
        "securityhub:BatchGetEnabledRegionsV2",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "security-ir:BatchGetMemberAccountDetails",
        "security-ir:GetCase",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:GetMembership",
        "security-ir:ListCaseEdits",
        "security-ir:ListCases",
        "security-ir:ListComments",
        "security-ir:ListInvestigations",
        "security-ir:ListMemberships",
        "security-ir:ListTagsForResource",
        "serverlessrepo:GetApplicationPolicy",
        "serverlessrepo:List*",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "servicequotas:ListTagsForResource",
        "ses:Describe*",
        "ses:GetAccount",
        "ses:GetAccountSendingEnabled",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetDedicatedIps",
        "ses:GetEmailIdentity",
        "ses:GetIdentityDkimAttributes",
```

```
        "ses:GetIdentityPolicies",
        "ses:GetIdentityVerificationAttributes",
        "ses:ListConfigurationSets",
        "ses:ListDedicatedIpPools",
        "ses:ListIdentities",
        "ses:ListIdentityPolicies",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListVerifiedEmailAddresses",
        "shield:Describe*",
        "shield:GetSubscriptionState",
        "shield:List*",
        "snowball:ListClusters",
        "snowball:ListJobs",
        "sns:GetDataProtectionPolicy",
        "sns:GetPlatformApplicationAttributes",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:Describe*",
        "ssm:GetAutomationExecution",
        "ssm:GetServiceSetting",
        "ssm:ListAssociations",
        "ssm:ListAssociationVersions",
        "ssm:ListCommands",
        "ssm:ListComplianceItems",
        "ssm:ListComplianceSummaries",
        "ssm:ListDocumentMetadataHistory",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "ssm:ListInventoryEntries",
        "ssm:ListOpsMetadata",
        "ssm:ListResourceComplianceSummaries",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso:DescribeAccountAssignmentCreationStatus",
        "sso:DescribeAccountAssignmentDeletionStatus",
```

```
        "sso:DescribeApplication",
        "sso:DescribeApplicationAssignment",
        "sso:DescribeApplicationProvider",
        "sso:DescribeInstance",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:DescribePermissionSetProvisioningStatus",
        "sso:DescribeRegion",
        "sso:DescribeTrustedTokenIssuer",
        "sso:GetApplicationAccessScope",
        "sso:GetApplicationAssignmentConfiguration",
        "sso:GetApplicationAuthenticationMethod",
        "sso:GetApplicationGrant",
        "sso:GetApplicationSessionConfiguration",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:ListAccountAssignmentCreationStatus",
        "sso:ListAccountAssignmentDeletionStatus",
        "sso:ListAccountAssignments",
        "sso:ListAccountAssignmentsForPrincipal",
        "sso:ListAccountsForProvisionedPermissionSet",
        "sso:ListApplicationAccessScopes",
        "sso:ListApplicationAssignments",
        "sso:ListApplicationAssignmentsForPrincipal",
        "sso:ListApplicationAuthenticationMethods",
        "sso:ListApplicationGrants",
        "sso:ListApplicationInstanceCertificates",
        "sso:ListApplicationInstances",
        "sso:ListApplicationProviders",
        "sso:ListApplications",
        "sso:ListApplicationTemplates",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListDirectoryAssociations",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSetProvisioningStatus",
        "sso:ListPermissionSets",
        "sso:ListPermissionSetsProvisionedToAccount",
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListRegions",
        "sso:ListTagsForResource",
        "sso:ListTrustedTokenIssuers",
        "sso-directory:ListExternalIdPConfigurationsForDirectory",
```

```
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "states:ListTagsForResource",
        "storagegateway:DescribeBandwidthRateLimit",
        "storagegateway:DescribeCache",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:DescribeMaintenanceStartTime",
        "storagegateway:DescribeNFSFileShares",
        "storagegateway:DescribeSMBSettings",
        "storagegateway:DescribeSnapshotSchedule",
        "storagegateway:DescribeStorediSCSIVolumes",
        "storagegateway:DescribeTapeArchives",
        "storagegateway:DescribeTapeRecoveryPoints",
        "storagegateway:DescribeTapes",
        "storagegateway:DescribeUploadBuffer",
        "storagegateway:DescribeVTLDevices",
        "storagegateway:DescribeWorkingStorage",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "tag:GetTagKeys",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts",
        "transcribe:GetCallAnalyticsCategory",
        "transcribe:GetMedicalVocabulary",
        "transcribe:GetVocabulary",
        "transcribe:GetVocabularyFilter",
        "transcribe:ListCallAnalyticsCategories",
```

```
        "transcribe:ListCallAnalyticsJobs",
        "transcribe:ListLanguageModels",
        "transcribe:ListMedicalTranscriptionJobs",
        "transcribe:ListMedicalVocabularies",
        "transcribe:ListTagsForResource",
        "transcribe:ListTranscriptionJobs",
        "transcribe:ListVocabularies",
        "transcribe:ListVocabularyFilters",
        "transfer:Describe*",
        "transfer:List*",
        "translate:List*",
        "trustedadvisor:Describe*",
        "voiceid:DescribeDomain",
        "waf-regional:GetWebACL",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:ListTagsForResource",
        "waf-regional:ListWebACLs",
        "waf:GetWebACL",
        "waf:ListTagsForResource",
        "waf:ListWebACLs",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:ListIPSets",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListResourcesForWebACL",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wafv2:ListWebACLs",
        "wisdom:GetAssistant",
        "wisdom:ListAssistants",
        "workdocs:DescribeResourcePermissions",
        "workspaces:Describe*",
        "xray:GetEncryptionConfig",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetTraceSummaries",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/cors",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/exports/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
```

```
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SecurityLakeResourceManagementServiceRolePolicy

Descrição: concede acesso para gerenciar os recursos criados pelo Security Lake.

`SecurityLakeResourceManagementServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 14 de novembro de 2024, 22:10 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeResourceManagementServiceRolePolicy`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadEventBridgeRules",
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AmazonSecurityLake-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeLambdaConfigurations",
      "Effect" : "Allow",
      "Action" : [
```

```
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:PutFunctionConcurrency",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetFunctionConcurrency",
        "lambda:GetRuntimeManagementConfig",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:PublishVersion",
        "lambda:DeleteFunctionConcurrency",
        "lambda:DeleteEventSourceMapping",
        "lambda:GetAlias",
        "lambda:GetPolicy",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeletePartitionUpdaterLambda",
      "Effect" : "Allow",
      "Action" : "lambda:DeleteFunction",
      "Resource" :
"arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListLambdaEventSourceMappings",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListEventSourceMappings"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowUpdateLambdaEventSourceMapping",
      "Effect" : "Allow",
      "Action" : [
        "lambda:UpdateEventSourceMapping"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "lambda:FunctionArn" :
 "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
        }
      }
    },
    {
      "Sid" : "AllowUpdateLambdaConfigs",
      "Effect" : "Allow",
      "Action" : [
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-
*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeGlueResources",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
```

```
        "glue:GetTables",
        "glue:UpdateTable",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDataLakeConfigurationManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObjectAttributes",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:GetEncryptionConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataCompactionAndManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:DeleteObject",
```

```
        "s3:RestoreObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReadSecurityLakeLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetQueryResults",
        "logs:GetLogRecord"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLakeMetastoreManager-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeSQSQueue",
      "Effect" : "Allow",
      "Action" : [
        "sqs:StartMessageMoveTask",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ChangeMessageVisibility",
        "sqs:ListMessageMoveTasks",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
```

```
        "sqs:SetQueueAttributes"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:SecurityLake_*",
        "arn:aws:sqs:*:*:AmazonSecurityLakeManager-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDataLakeManagement",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SecurityLakeServiceLinkedRole

Descrição: esta política concede permissões para operar o serviço Amazon Security Lake em seu nome

`SecurityLakeServiceLinkedRole` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 29 de novembro de 2022, 14:03 UTC
- Horário editado: 15 de julho de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsPolicies",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeOrgAccounts",
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/o-*/*"
      ]
    },
    {
      "Sid" : "AllowManagementOfServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel",
        "cloudtrail:GetServiceLinkedChannel",
        "cloudtrail:UpdateServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-lake/*"
    },
    {
      "Sid" : "AllowListServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationTrailValidation",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeAnyVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "ListDelegatedAdmins",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowWafLoggingConfiguration",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "wafv2:LogScope" : "SecurityLake"
        }
      }
    },
    {
      "Sid" : "AllowPutLoggingConfiguration",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "wafv2:LogDestinationResource" : "arn:aws:s3:::aws-waf-logs-security-lake-*"
        }
      }
    },
    {
```

```
      "Sid" : "ListWebACLs",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:ListWebACLs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ServerMigration_ServiceRole

Descrição: Permissões para permitir que o Serviço de Migração AWS do Servidor migre VMs para o EC2: permite que o Serviço de Migração do Servidor coloque os recursos migrados na conta EC2 do cliente.

`ServerMigration_ServiceRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ServerMigration_ServiceRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 11 de agosto de 2020, 20:41 UTC
- Hora da edição: 15 de outubro de 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*",
      "Condition" : {
        "Null" : {
          "cloudformation:ResourceTypes" : "false"
        },
        "ForAllValues:StringEquals" : {
          "cloudformation:ResourceTypes" : [
            "AWS::EC2::Instance",
            "AWS::ApplicationInsights::Application",
            "AWS::ResourceGroups::Group"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::sms-app-*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "sms:CreateReplicationJob",
        "sms:DeleteReplicationJob",
        "sms:GetReplicationJobs",
        "sms:GetReplicationRuns",
        "sms:GetServers",
        "sms:ImportServerCatalog",
        "sms:StartOnDemandReplicationRun",
        "sms:UpdateReplicationJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:s3:::sms-app-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/UseForSMSApplicationValidation" : [
            "true"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
```

```
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DeregisterImage",
        "ec2:ImportImage",
```

```
        "ec2:DescribeImportImageTasks",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
```

```
          "iam:PassedToService" : "cloudformation.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ServerMigrationConnector

Descrição: Permissões para permitir que o AWS Server Migration Connector migre VMs para o EC2. Permite a comunicação com o AWS Server Migration Service, o read/write acesso aos buckets do S3 começando com 'sms-b-' e 'import-to-ec2-', bem como aos buckets usados para atualização do Server Migration Connector, AWS registro AWS do Server Migration Connector com e upload de métricas para. AWS AWS

`ServerMigrationConnector` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ServerMigrationConnector` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de outubro de 2016, 21:45 UTC
- Hora da edição: 24 de outubro de 2016, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:SendMessage",
        "sms:GetMessages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::sms-b-*",
        "arn:aws:s3:::import-to-ec2-*",
        "arn:aws:s3:::server-migration-service-upgrade",
        "arn:aws:s3:::server-migration-service-upgrade/*",
        "arn:aws:s3:::connector-platform-upgrade-info/*",
        "arn:aws:s3:::connector-platform-upgrade-info",
        "arn:aws:s3:::connector-platform-upgrade-bundles/*",
        "arn:aws:s3:::connector-platform-upgrade-bundles",
        "arn:aws:s3:::connector-platform-release-notes/*",
        "arn:aws:s3:::connector-platform-release-notes"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "awsconnector:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ServerMigrationServiceConsoleFullAccess

Descrição: permissões necessárias para usar todos os recursos do Server Migration Service Console

`ServerMigrationServiceConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ServerMigrationServiceConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 09 de maio de 2020, 17:18 UTC
- Hora da edição: 20 de julho de 2020, 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sms:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
```

```
    },
    {
      "Action" : "s3:ListAllMyBuckets",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "sms.amazonaws.com"
        }
      },
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ServerMigrationServiceLaunchRole

Descrição: Permissões para permitir que o Serviço de Migração de AWS Servidores crie e atualize AWS recursos relevantes no cliente Conta da AWS para iniciar servidores e aplicativos migrados.

`ServerMigrationServiceLaunchRole` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ServerMigrationServiceLaunchRole` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 26 de novembro de 2018, 19:53 UTC
- Hora da edição: 15 de outubro de 2020, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:CreateApplication",
        "applicationinsights:CreateComponent",
        "applicationinsights:UpdateApplication",
        "applicationinsights:DeleteApplication",
        "applicationinsights:UpdateComponentConfiguration",
        "applicationinsights:DeleteComponent"
      ],
      "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
```

```
        "resource-groups:UpdateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ServerMigrationServiceRoleForInstanceValidation

Descrição: Permissões para permitir que o AWS SMS execute o script de validação de dados usado e envie o script de success/failure volta ao SMS

`ServerMigrationServiceRoleForInstanceValidation` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ServerMigrationServiceRoleForInstanceValidation` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 20 de julho de 2020, 22:25 UTC
- Hora da edição: 20 de julho de 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ServiceQuotasFullAccess

Descrição: fornece acesso total ao Service Quotas

`ServiceQuotasFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ServiceQuotasFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de junho de 2019, 15:44 UTC
- Hora da edição: 04 de fevereiro de 2021, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "dynamodb:DescribeLimits",
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "servicequotas:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/ServiceQuotaMonitor" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "servicequotas.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ServiceQuotasReadOnlyAccess

Descrição: fornece acesso somente de leitura ao Service Quotas

`ServiceQuotasReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ServiceQuotasReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 24 de junho de 2019, 15:31 UTC
- Horário editado: 12 de fevereiro de 2026, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "dynamodb:DescribeLimits",
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",
        "tag:GetTagValues",
```

```
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServices",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListTagsForResource",
        "servicequotas:GetAutoManagementConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:GetNotificationConfiguration",
        "notifications:GetEventRule",
        "notifications:ListNotificationHubs",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:GetEmailContact",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chatbot:DescribeChimeWebhookConfigurations",
        "chatbot:DescribeSlackChannelConfigurations",
        "consoleapp:ListDeviceIdentities",
        "consoleapp:GetDeviceIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ServiceQuotasServiceRolePolicy

Descrição: permite que o Service Quotas crie casos de suporte em seu nome

`ServiceQuotasServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário da criação: 22 de maio de 2019, 20:44 UTC
- Hora da edição: 24 de junho de 2019, 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SignInLocalDevelopmentAccess

Descrição: fornece permissões para acesso programático por AWS meio do AWS Sign-in serviço, incluindo a criação de tokens OAuth2 para ferramentas e aplicativos de desenvolvedores.

`SignInLocalDevelopmentAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SignInLocalDevelopmentAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 19 de novembro de 2025, 18:34 UTC
- Horário editado: 12 de fevereiro de 2026, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/SignInLocalDevelopmentAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "signin:AuthorizeOAuth2Access",
        "signin:CreateOAuth2Token"
      ],
      "Resource" : "arn:aws:signin:*:*:oauth2/public-client/*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SimpleWorkflowFullAccess

Descrição: fornece acesso total ao serviço de configuração do Simple Workflow.

`SimpleWorkflowFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SimpleWorkflowFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 06 de fevereiro de 2015, 18:41 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:41 UTC

- ARN: `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "swf:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SMSVoiceServiceRolePolicy

Descrição: Permite que o SMSVoice publique métricas CloudWatch em seu nome

`SMSVoiceServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Horário de criação: 14 de novembro de 2024, 17:04 UTC
- Horário editado: 14 de novembro de 2024, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SMSVoiceServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/SMSVoice"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SplitCostAllocationDataServiceRolePolicy

Descrição: permite que dados de alocação de custo dividido recuperem informações da AWS organização, se aplicável, e coletem dados de telemetria para os serviços de dados de alocação de custos divididos que o cliente optou por usar.

`SplitCostAllocationDataServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 16 de abril de 2024, 16:05 UTC
- Hora da edição: 16 de abril de 2024, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SplitCostAllocationDataServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListParents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonManagedServiceForPrometheusAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:ListWorkspaces",
        "aps:QueryMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SSMQuickSetupRolePolicy

Descrição: fornece permissões para verificar a integridade da Configuração Rápida, garantir o uso uniforme dos parâmetros e dos recursos provisionados e corrigir os recursos quando o desvio é detectado.

`SSMQuickSetupRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 25 de junho de 2024, 15:20 UTC
- Horário editado: 18 de novembro de 2024, 13:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SSMQuickSetupRolePolicy`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SSMResourceDataSyncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListResourceDataSync"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMResourceDataSyncGetOpsSummaryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsSummary"
      ],
```

```
      "Resource" : "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*"
    },
    {
      "Sid" : "SSMResourceDataSyncManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteResourceDataSync"
      ],
      "Resource" : "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*",
      "Condition" : {
        "StringEquals" : {
          "ssm:SyncType" : "SyncFromSource"
        }
      }
    },
    {
      "Sid" : "SSMAssociationsReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListAssociations",
        "ssm:DescribeAssociationExecutions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QuickSetupSSMDocumentsReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-*",
        "arn:aws:ssm:*:*:document/*-AWSQuickSetupType-*"
      ]
    },
    {
      "Sid" : "OrganizationReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
```

```
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedServicesForAccount"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QuickSetupStackSetReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults",
        "cloudformation:GetTemplate"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset/SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SSMQuickSetup*"
      ]
    },
    {
      "Sid" : "QuickSetupStackSetDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset/SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset-target/SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:type/resource/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "QuickSetupCfnStacksDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SupportUser

Descrição: esta política concede permissões para solucionar e resolver problemas em uma Conta da AWS. Essa política também permite que o usuário entre em contato com o AWS suporte para criar e gerenciar casos.

`SupportUser` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SupportUser` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de trabalho
- Hora da criação: 10 de novembro de 2016, 17:21 UTC
- Horário editado: 12 de fevereiro de 2026, 18:03 UTC

- ARN: `arn:aws:iam::aws:policy/job-function/SupportUser`

Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*",
        "acm:DescribeCertificate",
        "acm:GetCertificate",
        "acm:List*",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities",
        "apigateway:GET",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:Describe*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:EstimateTemplateCost",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents",
        "cloudtrail:ListTags",
        "cloudtrail:ListPublicKeys",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
```

```
        "codecommit:BatchGetRepositories",
        "codecommit:Get*",
        "codecommit:List*",
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:AcknowledgeJob",
        "codepipeline:AcknowledgeThirdPartyJob",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:PollForJobs",
        "codepipeline:PollForThirdPartyJobs",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipeline",
        "cognito-identity:List*",
        "cognito-identity:LookupDeveloperIdentity",
        "cognito-identity:Describe*",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeRiskConfiguration",
        "cognito-idp:DescribeUserImportJob",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:List*",
        "cognito-sync:Describe*",
        "cognito-sync:GetBulkPublishDetails",
        "cognito-sync:GetCognitoEvents",
        "cognito-sync:GetIdentityPoolConfiguration",
        "cognito-sync:List*",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetResourceConfigHistory",
        "config:ListDiscoveredResources",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "datapipeline:ReportTaskProgress",
        "datapipeline:ReportTaskRunnerHeartbeat",
        "devicefarm:List*",
```

```
        "devicefarm:Get*",
        "directconnect:Describe*",
        "discovery:Describe*",
        "discovery:ListConfigurations",
        "dms:Describe*",
        "dms:List*",
        "ds:DescribeDirectories",
        "ds:DescribeSnapshots",
        "ds:GetDirectoryLimits",
        "ds:GetSnapshotLimits",
        "ds:ListAuthorizedApplications",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:Describe*",
        "ec2:DescribeHosts",
        "ec2:describeIdentityIdFormat",
        "ec2:DescribeIdFormat",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeNatGateways",
        "ec2:DescribeReservedInstancesModifications",
        "ec2:DescribeTags",
        "ec2:SearchLocalGatewayRoutes",
        "ecr:GetRepositoryPolicy",
        "ecr:BatchCheckLayerAvailability",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticbeanstalk:ValidateConfigurationSettings",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elastictranscoder:List*",
        "elastictranscoder:ReadJob",
        "elasticfilesystem:DescribeFileSystems",
```

```
        "es:Describe*",
        "es:List*",
        "es:ESHttpGet",
        "es:ESHttpHead",
        "events:DescribeRule",
        "events:List*",
        "events:TestEventPattern",
        "firehose:Describe*",
        "firehose:List*",
        "gamelift:List*",
        "gamelift:Describe*",
        "glacier:ListVaults",
        "glacier:DescribeVault",
        "glacier:DescribeJob",
        "glacier:Get*",
        "glacier:List*",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "importexport:GetStatus",
        "importexport:ListJobs",
        "inspector:Describe*",
        "inspector:List*",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:DiscoverInputSchema",
        "kinesisanalytics:GetApplicationState",
        "kinesisanalytics:ListApplications",
        "kinesis:Describe*",
        "kinesis:Get*",
        "kinesis:List*",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lambda:List*",
        "lambda:Get*",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "machinelearning:Describe*",
        "machinelearning:Get*",
        "opsworks:Describe*",
```

```
        "rds:Describe*",
        "rds:ListTagsForResource",
        "redshift:Describe*",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53:Get*",
        "route53:List*",
        "route53domains:CheckDomainAvailability",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:List*",
        "s3:List*",
        "sdb:GetAttributes",
        "sdb:List*",
        "sdb:Select*",
        "servicecatalog:SearchProducts",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ScanProvisionedProducts",
        "ses:Get*",
        "ses:List*",
        "sns:Get*",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListQueues",
        "sqs:ReceiveMessage",
        "ssm:List*",
        "ssm:Describe*",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "swf:Count*",
        "swf:Describe*",
```

```
        "swf:Get*",
        "swf:List*",
        "waf:Get*",
        "waf:List*",
        "workdocs:Describe*",
        "workmail:Describe*",
        "workmail:Get*",
        "workspaces:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

SystemAdministrator

Descrição: concede permissões de acesso total necessárias aos recursos necessários para operações de aplicações e desenvolvimento.

`SystemAdministrator` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `SystemAdministrator` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de trabalho
- Hora da criação: 10 de novembro de 2016, 17:23 UTC
- Horário editado: 12 de fevereiro de 2026, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SystemAdministrator`

Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Statement" : [
    {
      "Action" : [
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "acm:Request*",
        "acm:Resend*",
        "autoscaling:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListPublicKeys",
        "cloudtrail:ListTags",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudwatch:*",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateBranch",
        "codecommit:CreateRepository",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:List*",
        "codecommit:Put*",
        "codecommit:Test*",
        "codecommit:Update*",
        "codedeploy:*",
        "codepipeline:*",
        "config:*",
        "ds:*",
        "ec2:Allocate*",
```

```
        "ec2:AssignPrivateIpAddresses*",
        "ec2:Associate*",
        "ec2:Allocate*",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:Bundle*",
        "ec2:Cancel*",
        "ec2:Copy*",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDhcpOptions",
        "ec2:CreateFlowLogs",
        "ec2:CreateImage",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreatePlacementGroup",
        "ec2:CreateReservedInstancesListing",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateSpotDatafeedSubscription",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteKeyPair",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteSpotDatafeedSubscription",
```

```
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DeregisterImage",
        "ec2:Describe*",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVolumeIO",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetConsoleOutput",
        "ec2:GetHostReservationPurchasePreview",
        "ec2:GetLaunchTemplateData",
        "ec2:GetPasswordData",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:Import*",
        "ec2:Modify*",
        "ec2:MonitorInstances",
        "ec2:MoveAddressToVpc",
        "ec2:Purchase*",
        "ec2:RegisterImage",
        "ec2:Release*",
        "ec2:Replace*",
        "ec2:ReportInstanceStatus",
        "ec2:Request*",
        "ec2:Reset*",
        "ec2:RestoreAddressToClassic",
        "ec2:RunScheduledInstances",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UnmonitorInstances",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "elasticloadbalancing:*",
        "events:*",
        "iam:GetAccount*",
```

```
        "iam:GetContextKeys*",
        "iam:GetCredentialReport",
        "iam:ListAccountAliases",
        "iam:ListGroups",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:Simulate*",
        "iam:UpdateServerCertificate",
        "iam:UpdateSigningCertificate",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms:DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "lambda:Create*",
        "lambda:Delete*",
        "lambda:Get*",
        "lambda:InvokeFunction",
        "lambda:List*",
        "lambda:PublishVersion",
        "lambda:Update*",
        "logs:*",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "rolesanywhere:PutNotificationSettings",
```

```
        "rolesanywhere:ResetNotificationSettings",
        "route53:*",
        "route53domains:*",
        "ses:*",
        "sns:*",
        "sqs:*",
        "trustedadvisor:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl*",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DetachClassicLinkVpc",
        "ec2:DetachVolume",
        "ec2:DisableVpcClassicLink",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
        "ec2:RebootInstances",
        "ec2:RejectVpcPeeringConnection",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Effect" : "Allow",
      "Resource" : [
```

```
      "*"
    ]
  },
  {
    "Action" : "s3:*",
    "Effect" : "Allow",
    "Resource" : [
      "*"
    ]
  },
  {
    "Action" : [
      "iam:GetAccessKeyLastUsed",
      "iam:GetGroup*",
      "iam:GetInstanceProfile",
      "iam:GetLoginProfile",
      "iam:GetOpenIDConnectProvider",
      "iam:GetPolicy*",
      "iam:GetRole*",
      "iam:GetSAMLProvider",
      "iam:GetSSHPublicKey",
      "iam:GetServerCertificate",
      "iam:GetServiceLastAccessed*",
      "iam:GetUser*",
      "iam:ListAccessKeys",
      "iam:ListAttached*",
      "iam:ListEntitiesForPolicy",
      "iam:ListGroupPolicies",
      "iam:ListGroupsForUser",
      "iam:ListInstanceProfiles*",
      "iam:ListMFADevices",
      "iam:ListPolicyVersions",
      "iam:ListRolePolicies",
      "iam:ListSSHPublicKeys",
      "iam:ListSigningCertificates",
      "iam:ListUserPolicies",
      "iam:Upload*"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "*"
    ]
  },
  {
```

```
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/rds-monitoring-role",
        "arn:aws:iam::*:role/ec2-sysadmin-*",
        "arn:aws:iam::*:role/ecr-sysadmin-*",
        "arn:aws:iam::*:role/lambda-sysadmin-*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

TranslateFullAccess

Descrição: fornece acesso total ao Amazon Translate.

`TranslateFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `TranslateFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 27 de novembro de 2018, 23:36 UTC
- Hora da edição: 08 de janeiro de 2020, 21:22 UTC

- ARN: `arn:aws:iam::aws:policy/TranslateFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "translate:*",
        "comprehend:DetectDominantLanguage",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

TranslateReadOnly

Descrição: fornece acesso somente leitura ao Amazon Translate.

`TranslateReadOnly` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `TranslateReadOnly` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2017, 18:22 UTC
- Hora da edição: 24 de maio de 2023, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "translate:TranslateText",
        "translate:TranslateDocument",
        "translate:GetTerminology",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
```

```
        "translate:ListParallelData",
        "comprehend:DetectDominantLanguage",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

ViewOnlyAccess

Descrição: Essa política concede permissões para visualizar recursos e metadados básicos em todos os AWS serviços.

`ViewOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `ViewOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de trabalho
- Hora da criação: 10 de novembro de 2016, 17:20 UTC
- Horário editado: 30 de setembro de 2026, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

Versão da política

Versão da política: v46 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralViewOnlyAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "aiops:GetInvestigation",
        "aiops:GetInvestigationGroup",
        "aiops:ListInvestigationEvents",
        "aiops:ListInvestigationGroups",
        "aiops:ListInvestigations",
        "amplify:GetWebACLForResource",
        "amplify:ListDomainAssociations",
        "amplify:ListResourcesForWebACL",
        "apigateway:GetPortal",
        "apigateway:GetPortalProduct",
        "apigateway:GetPortalProductSharingPolicy",
        "apigateway:GetRoutingRule",
        "apigateway:ListPortalProducts",
        "apigateway:ListPortals",
        "apigateway:ListProductPages",
        "apigateway:ListProductRestEndpointPages",
        "apigateway:ListRoutingRules",
        "appconfig:GetAccountSettings",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExperimentDefinition",
        "appconfig:GetExtension",
        "appconfig:GetExtensionAssociation",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListDeployments",
```

```
        "appconfig:ListEnvironments",
        "appconfig:ListExperimentDefinitions",
        "appconfig:ListExperimentRuns",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appsync:GetApi",
        "appsync:GetChannelNamespace",
        "appsync:GetGraphqlApi",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResourcePolicy",
        "appsync:GetSourceApiAssociation",
        "athena:List*",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "backup:DescribeBackupJob",
        "backup:DescribeBackupVault",
        "backup:DescribeCopyJob",
        "backup:DescribeFramework",
        "backup:DescribeGlobalSettings",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeRegionSettings",
        "backup:DescribeReportJob",
        "backup:DescribeReportPlan",
        "backup:DescribeRestoreJob",
        "backup:GetBackupPlan",
        "backup:GetBackupPlanFromJSON",
        "backup:GetBackupPlanFromTemplate",
        "backup:GetBackupSelection",
        "backup:GetSupportedResourceTypes",
        "backup:ListBackupJobs",
        "backup:ListBackupPlans",
        "backup:ListBackupPlanTemplates",
        "backup:ListBackupPlanVersions",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListCopyJobs",
        "backup:ListFrameworks",
        "backup:ListLegalHolds",
        "backup:ListProtectedResources",
        "backup:ListProtectedResourcesByBackupVault",
        "backup:ListRecoveryPointsByBackupVault",
```

```
        "backup:ListRecoveryPointsByLegalHold",
        "backup:ListRecoveryPointsByResource",
        "backup:ListReportJobs",
        "backup:ListReportPlans",
        "backup:ListRestoreJobs",
        "backup:ListTags",
        "batch:ListJobs",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetResourcePolicy",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock:GetAccountDataRetention",
        "bedrock:GetAdvancedPromptOptimizationJob",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:GetAsyncInvoke",
        "bedrock:GetAutomatedReasoningPolicy",
        "bedrock:GetAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:GetAutomatedReasoningPolicyNextScenario",
        "bedrock:GetBlueprint",
        "bedrock:GetBlueprintOptimizationStatus",
        "bedrock:GetBlueprintRecommendation",
        "bedrock:GetCustomModel",
        "bedrock:GetCustomModelDeployment",
        "bedrock:GetDataAutomationLibrary",
        "bedrock:GetDataAutomationLibraryIngestionJob",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataAutomationStatus",
        "bedrock:GetDataSource",
        "bedrock:GetEvaluationJob",
        "bedrock:GetExecutionFlowSnapshot",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowExecution",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
```

```
        "bedrock:GetGuardrail",
        "bedrock:GetImportedModel",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestedDocumentAcl",
        "bedrock:GetIngestionJob",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetKnowledgeBaseDocuments",
        "bedrock:GetMarketplaceModelEndpoint",
        "bedrock:GetModelCopyJob",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationJob",
        "bedrock:GetResourcePolicy",
        "bedrock:ListCustomModels",
        "bedrock:ListTagsForResource",
        "clouddirectory:ListAppliedSchemaArns",
        "clouddirectory:ListDevelopmentSchemaArns",
        "clouddirectory:ListDirectories",
        "clouddirectory:ListPublishedSchemaArns",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplateSummary",
        "cloudformation:List*",
        "cloudfront:List*",
        "cloudsearch:DescribeDomains",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codebuild:ListBuilds*",
        "codebuild:ListProjects",
        "codecommit:List*",
        "codedeploy:BatchGetApplicationRevisions",
        "codedeploy:BatchGetApplications",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:BatchGetDeploymentInstances",
        "codedeploy:BatchGetDeployments",
        "codedeploy:BatchGetDeploymentTargets",
        "codedeploy:BatchGetOnPremisesInstances",
        "codedeploy:Get*",
        "codedeploy:List*",
```

```
        "codepipeline:ListPipelines",
        "codestar:List*",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentities",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:List*",
        "cognito-sync:ListDatasets",
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:List*",
        "connect:List*",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetAccountLimits",
        "datapipeline:ListPipelines",
        "dax:DescribeClusters",
        "dax:DescribeDefaultParameters",
        "dax:DescribeEvents",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "devicefarm:List*",
        "directconnect:Describe*",
        "discovery:List*",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "dlm:ListTagsForResource",
        "dms:List*",
        "ds:DescribeDirectories",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeEndpoints",
        "dynamodb:DescribeExport",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
```

```
        "dynamodb:DescribeImport",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetAbacStatus",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListBackups",
        "dynamodb:ListContributorInsights",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListImports",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAccountVpcEncryptionControl",
        "ec2:DescribeAddressTransfers",
        "ec2:DescribeAddresses",
        "ec2:DescribeAddressesAttribute",
        "ec2:DescribeAggregateIdFormat",
        "ec2:DescribeApplicationStatus",
        "ec2:DescribeApplicationStatusCheckAssociations",
        "ec2:DescribeApplicationStatusChecks",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAwsNetworkPerformanceMetricSubscriptions",
        "ec2:DescribeBundleTasks",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeCapacityBlockExtensionHistory",
        "ec2:DescribeCapacityBlockExtensionOfferings",
        "ec2:DescribeCapacityBlockOfferings",
        "ec2:DescribeCapacityBlockStatus",
        "ec2:DescribeCapacityBlocks",
        "ec2:DescribeCapacityManagerDataExports",
        "ec2:DescribeCapacityReservationBillingRequests",
        "ec2:DescribeCapacityReservationCancellationQuotes",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservationTopology",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
```

```
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeClientVpnAuthorizationRules",
        "ec2:DescribeClientVpnConnections",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeClientVpnRoutes",
        "ec2:DescribeClientVpnTargetNetworks",
        "ec2:DescribeCoipPools",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDeclarativePoliciesReports",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFastLaunchImages",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImageAttribute",
        "ec2:DescribeFpgaImages",
        "ec2:DescribeHost*",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeIdentityIdFormat",
        "ec2:DescribeIdFormat",
        "ec2:DescribeImage*",
        "ec2:DescribeImport*",
        "ec2:DescribeInstance*",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamByoasn",
        "ec2:DescribeIpamExternalResourceVerificationTokens",
        "ec2:DescribeIpamInternetRegistryAssociations",
        "ec2:DescribeIpamPolicies",
        "ec2:DescribeIpamPoolAllocations",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpamPrefixListResolverTargets",
        "ec2:DescribeIpamPrefixListResolvers",
        "ec2:DescribeIpamResourceDiscoveries",
        "ec2:DescribeIpamResourceDiscoveryAssociations",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeIpams",
        "ec2:DescribeIpv6Pools",
```

```
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLockedSnapshots",
        "ec2:DescribeMacHosts",
        "ec2:DescribeMacModificationTasks",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetwork*",
        "ec2:DescribeOutpostLags",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribePrincipalIdFormat",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeRegions",
        "ec2:DescribeReplaceRootVolumeTasks",
        "ec2:DescribeReserved*",
        "ec2:DescribeRouteServerEndpoints",
        "ec2:DescribeRouteServerPeers",
        "ec2:DescribeRouteServers",
        "ec2:DescribeRouteTables",
        "ec2:DescribeScheduledInstanceAvailability",
        "ec2:DescribeScheduledInstances",
        "ec2:DescribeSecondaryInterfaces",
        "ec2:DescribeSecondaryNetworks",
        "ec2:DescribeSecondarySubnets",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeServiceLinkVirtualInterfaces",
        "ec2:DescribeSnapshot*",
        "ec2:DescribeSpot*",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeStoreImageTasks",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilterRules",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayMeteringPolicies",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTrunkInterfaceAssociations",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstanceLoggingConfigurations",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolume*",
        "ec2:DescribeVpc*",
        "ec2:DescribeVpnConcentrators",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetActiveVpnTunnelStatus",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetAssociatedIpv6PoolCidrs",
        "ec2:GetCapacityManagerAttributes",
        "ec2:GetCapacityManagerMetricDimensions",
        "ec2:GetCapacityManagerMonitoredTagKeys",
        "ec2:GetCapacityReservationUsage",
        "ec2:GetCoipPoolUsage",
        "ec2:GetDeclarativePoliciesReportSummary",
        "ec2:GetDefaultCreditSpecification",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEnabledIpamPolicy",
        "ec2:GetFlowLogsIntegrationTemplate",
        "ec2:GetGroupsForCapacityReservation",
```

```
        "ec2:GetHostReservationPurchasePreview",
        "ec2:GetImageAncestry",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetInstanceMetadataDefaults",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamAddressHistory",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "ec2:GetIpamDiscoveredRoutes",
        "ec2:GetIpamInternetRegistryAssociationAsns",
        "ec2:GetIpamInternetRegistryAssociationCidrs",
        "ec2:GetIpamPolicyAllocationRules",
        "ec2:GetIpamPolicyOrganizationTargets",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetIpamPrefixListResolverRules",
        "ec2:GetIpamPrefixListResolverVersions",
        "ec2:GetIpamResourceCidrs",
        "ec2:GetIpamRouteOriginAuthorizations",
        "ec2:GetIpamRouteProtectionFindings",
        "ec2:GetIpamRoutingPolicyRegistrations",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedResourceVisibility",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetReservedInstancesExchangeQuote",
        "ec2:GetResourcePolicy",
        "ec2:GetRouteServerAssociations",
        "ec2:GetRouteServerPropagations",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetSpotPlacementScores",
        "ec2:GetSubnetCidrReservations",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayMeteringPolicyEntries",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:GetTransitGatewayPolicyTableEntries",
        "ec2:GetTransitGatewayPrefixListReferences",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessEndpointTargets",
```

```
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:GetVpcResourcesBlockingEncryptionEnforcement",
        "ec2:GetVpnConnectionDeviceTypes",
        "ec2:GetVpnTunnelReplacementStatus",
        "ec2:ListImagesInRecycleBin",
        "ec2:ListSnapshotsInRecycleBin",
        "ec2:ListVolumesInRecycleBin",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:SearchTransitGatewayRoutes",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeAddonConfiguration",
        "eks:DescribeAddonVersions",
        "eks:DescribeCapability",
        "eks:DescribeCluster",
        "eks:DescribeClusterVersions",
        "eks:DescribeEksAnywhereSubscription",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeInsight",
        "eks:DescribeInsightsRefresh",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:DescribeUpdate",
        "eks:ListAccessEntries",
        "eks:ListAccessPolicies",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListCapabilities",
        "eks:ListClusters",
        "eks:ListEksAnywhereSubscriptions",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListInsights",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "eks:ListTagsForResource",
```

```
        "eks:ListUpdates",
        "elasticache:Describe*",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticbeanstalk:ListAvailableSolutionStacks",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:List*",
        "elastictranscoder:List*",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:ListApplications",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:ListDomainNames",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "firehose:DescribeDeliveryStream",
        "firehose:List*",
        "fsx:DescribeFileSystems",
        "gamelift:List*",
        "glacier:DescribeJob",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultNotifications",
        "glacier:List*",
        "glue:GetJobRuns",
        "glue:GetResourcePolicies",
        "glue:GetSchema",
        "glue:GetTable",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:GetTags",
        "glue:ListJobs",
        "glue:ListSchemaVersions",
        "glue:ListSchemas",
        "glue:ListSessions",
```

```
        "greengrass:List*",
        "iam:GetAccountSummary",
        "iam:GetLoginProfile",
        "iam:List*",
        "importexport:ListJobs",
        "inspector:List*",
        "iot:List*",
        "kafka:ListClusters",
        "kendra:ListDataSources",
        "kendra:ListTagsForResource",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetResourcePolicy",
        "lambda:List*",
        "lex:GetBotAliases",
        "lex:GetBotChannelAssociations",
        "lex:GetBots",
        "lex:GetBotVersions",
        "lex:GetIntents",
        "lex:GetIntentVersions",
        "lex:GetSlotTypes",
        "lex:GetSlotTypeVersions",
        "lex:GetUtterancesView",
        "lightsail:GetBlueprints",
        "lightsail:GetBundles",
        "lightsail:GetInstances",
        "lightsail:GetInstancePortStates",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetKeyPair",
        "lightsail:GetRegions",
        "lightsail:GetStaticIps",
        "lightsail:IsVpcPeered",
        "logs:Describe*",
        "logs:GetTransformer",
        "logs:ListEntitiesForLogGroup",
        "logs:ListLogGroupsForEntity",
        "logs:ListLogGroupsForQuery",
        "logs:ListTagsForResource",
        "lookoutvision:ListModelPackagingJobs",
```

```
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:Describe*",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:ListRouterInputs",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListRouterNetworkInterfaces",
        "mediastore:DescribeContainer",
        "mediastore:GetLifecyclePolicy",
        "mediastore:ListTagsForResource",
        "memorydb:DescribeAcls",
        "memorydb:DescribeUsers",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetImportJobs",
        "mobiletargeting:GetSegments",
        "oam:ListAttachedLinks",
        "oam:ListLinks",
        "oam:ListSinks",
        "opsworks-cm:Describe*",
        "opsworks:Describe*",
        "organizations:List*",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites",
        "outposts:ListTagsForResource",
        "polly:Describe*",
        "polly:List*",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "qapps:GetQApp",
        "qapps:ListQApps",
        "qapps:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
```

```
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetPolicy",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "ram:GetResourceShareAssociations",
        "rds:Describe*",
        "redshift-serverless:GetResourcePolicy",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters",
        "redshift:DescribeEvents",
        "redshift:ViewQueriesInConsole",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53:Get*",
        "route53:List*",
        "route53domains:List*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sdb:List*",
        "servicecatalog:List*",
```

```
        "ses:DescribeActiveReceiptRuleSet",
        "ses:List*",
        "ses:ListDedicatedIpPools",
        "shield:List*",
        "sns:GetDataProtectionPolicy",
        "sns:GetSubscriptionAttributes",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "states:ListActivities",
        "states:ListExecutions",
        "states:ListMapRuns",
        "states:ListStateMachineAliases",
        "states:ListStateMachines",
        "states:ListStateMachineVersions",
        "storagegateway:DescribeSMBSettings",
        "storagegateway:ListGateways",
        "storagegateway:ListLocalDisks",
        "storagegateway:ListVolumeRecoveryPoints",
        "storagegateway:ListVolumes",
        "swf:List*",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts",
        "trustedadvisor:Describe*",
        "uxc:GetAccountCustomizations",
        "uxc:ListServices",
        "waf-regional:List*",
        "waf:List*",
        "wafv2:List*",
        "wisdom:ListAssistants",
        "workdocs:DescribeAvailableDirectories",
        "workdocs:DescribeInstances",
        "workmail:Describe*",
        "workspaces:Describe*",
        "xray:GetEncryptionConfig",
        "xray:GetGroups",
        "xray:GetSamplingRules",
```

```
        "xray:GetSamplingStatisticSummaries",
        "xray:GetSamplingTargets",
        "xray:GetTraceSegmentDestination",
        "xray:ListResourcePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/cors",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/exports/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
```

```
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

VMImportExportRoleForAWSConnector

Descrição: política padrão para a função de Import/Export serviço de VM, para clientes que usam o AWS Connector. O Import/Export serviço de VM assume uma função com essa política para atender às solicitações de migração de máquinas virtuais do dispositivo virtual AWS Connector. (Observe que o AWS Connector usa a política gerenciada “AWSconnector” para emitir solicitações em nome do cliente para o serviço de VM Import/Export .) Fornece a capacidade de criar AMIs e instantâneos do EBS, modificar atributos de instantâneos do EBS, fazer chamadas “Describe*” em objetos do EC2 e ler os buckets do S3 começando com “importar para ec2”.

`VMImportExportRoleForAWSConnector` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `VMImportExportRoleForAWSConnector` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: Política de função de serviço
- Hora da criação: 03 de setembro de 2015, 20:48 UTC
- Hora da edição: 03 de setembro de 2015, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::import-to-ec2-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:CopySnapshot",
        "ec2:RegisterImage",
        "ec2:Describe*"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

VPCLatticeFullAccess

Descrição: fornece acesso total ao Amazon VPC Lattice e acesso aos serviços de dependência.

`VPCLatticeFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `VPCLatticeFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de março de 2023, 2:49 UTC
- Horário editado: 12 de fevereiro de 2026, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "logs:DescribeLogGroups",
        "s3:ListAllMyBuckets",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:UpdateLogDelivery",
        "logs:DescribeResourcePolicies"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "vpc-lattice.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

VPCLatticeReadOnlyAccess

Descrição: Fornece acesso somente para leitura ao Amazon VPC Lattice por meio do Console de gerenciamento da AWS e acesso limitado aos serviços de dependência.

`VPCLatticeReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `VPCLatticeReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de março de 2023, 2:47 UTC
- Horário editado: 12 de fevereiro de 2026, 17:58 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:Get*",
        "vpc-lattice:List*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "logs:DescribeLogGroups",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "s3:ListAllMyBuckets",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

VPCLatticeServicesInvokeAccess

Descrição: esta política fornece acesso à invocação de serviços do Amazon VPC Lattice.

`VPCLatticeServicesInvokeAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `VPCLatticeServicesInvokeAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 30 de março de 2023, 2:45 UTC
- Hora da edição: 30 de março de 2023, 2:45 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice-svcs:Invoke"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

WAFLoggingServiceRolePolicy

Descrição: criar SLR para gravar os logs do cliente em um fluxo do Firehose

`WAFLoggingServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 24 de agosto de 2018, 21:05 UTC
- Horário editado: 20 de maio de 2026, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "KMSForFirehoseSSECMK",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "firehose.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

WAFRegionalLoggingServiceRolePolicy

Descrição: criar SLR para gravar os logs do cliente em um fluxo do Firehose

`WAFRegionalLoggingServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 24 de agosto de 2018, 18:40 UTC
- Horário editado: 20 de maio de 2026, 18:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
```

```
    {
      "Sid" : "KMSForFirehoseSSECMK",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "firehose.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

WAFV2LoggingServiceRolePolicy

Descrição: Essa política cria uma função vinculada ao serviço que permite ao AWS WAF gravar registros no Amazon Kinesis Data Firehose.

`WAFV2LoggingServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

Detalhes desta política

- Tipo: política de Service-linked função
- Hora da criação: 7 de novembro de 2019, 0:40 UTC

- Horário editado: 20 de maio de 2026, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FirehoseAPIStatement",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "DescribeOrganizationAPIStatement",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSForFirehoseSSECMK",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "firehose.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Saiba mais

- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

WellArchitectedAgentResourceScanning

Descrição: Concede ao AWS Well-Architected agente acesso somente para leitura às configurações de AWS recursos, configurações de segurança e dados operacionais para gerar recomendações de otimização

`WellArchitectedAgentResourceScanning` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `WellArchitectedAgentResourceScanning` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 16 de julho de 2026, 20:27 UTC
- Horário editado: 30 de setembro de 2026, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedAgentResourceScanning`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudControlDiscoveryCompact",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:List*",
        "acm-pca:Describe*",
        "acm-pca:Get*",
        "acm-pca:List*",
        "acm:DescribeCertificate",
        "aco-automation:GetAutomationRule",
        "aco-automation:ListAutomationRules",
        "aidevops:DescribePrivateConnection",
        "aidevops:Get*",
        "aidevops:List*",
        "aiops:Get*",
        "aiops:List*",
        "airflow-serverless:GetWorkflow",
        "airflow-serverless:List*",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "amplify:Get*",
        "amplify:List*",
        "amplifyuibuilder:Get*",
        "amplifyuibuilder:List*",
        "apigateway:GetRoutingRule",
        "apigateway:ListRoutingRules",
        "app-integrations:Get*",
        "app-integrations:List*",
        "appconfig:Get*",
        "appconfig:List*",
        "appflow:Describe*",
        "appflow:List*",
        "application-autoscaling:Describe*",
```

```
        "application-signals:GetServiceLevelObjective",
        "application-signals:List*",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "apprunner:Describe*",
        "apprunner:List*",
        "appstream:Describe*",
        "appstream:List*",
        "apptest:GetTestCase",
        "apptest:List*",
        "aps:Describe*",
        "aps:List*",
        "arc-region-switch:GetPlan",
        "arc-region-switch:List*",
        "arc-zonal-shift:Get*",
        "arc-zonal-shift:ListManagedResources",
        "athena:Get*",
        "athena:List*",
        "auditmanager:GetAssessment",
        "auditmanager:List*",
        "autoscaling:Describe*",
        "aws-external-anthropic:GetWorkspace",
        "aws-external-anthropic:List*",
        "b2bi:Get*",
        "b2bi:List*",
        "backup-gateway:GetHypervisor",
        "backup-gateway:List*",
        "backup:Describe*",
        "backup:Get*",
        "backup:List*",
        "batch:Describe*",
        "batch:List*",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:List*",
        "bcm-pricing-calculator:GetBillScenario",
        "bcm-pricing-calculator:List*",
        "bedrock-agentcore:Get*",
        "bedrock-agentcore:List*",
        "bedrock-mantle:GetProject",
        "bedrock-mantle:List*",
        "bedrock:Get*",
        "bedrock:List*",
        "billing:GetBillingView",
        "billing:List*",
```

```
        "billingconductor:List*",
        "braket:ListTagsForResource",
        "braket:Search*",
        "budgets:Describe*",
        "budgets:ListTagsForResource",
        "ce:DescribeCostCategoryDefinition",
        "ce:Get*",
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageWithResources",
        "ce:List*",
        "chatbot:Describe*",
        "chatbot:Get*",
        "chatbot:List*",
        "chime:Describe*",
        "chime:List*",
        "cleanrooms-ml:Get*",
        "cleanrooms-ml:List*",
        "cleanrooms:Get*",
        "cleanrooms:List*",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListTypes",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudtrail:Describe*",
        "cloudtrail:Get*",
        "cloudtrail:List*",
        "cloudwatch:Describe*",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:Get*",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricWidgetImage",
        "cloudwatch:List*",
        "cloudwatch:ListMetrics",
        "codeartifact:Describe*",
        "codeartifact:Get*",
        "codeartifact:List*",
        "codebuild:BatchGetFleets",
        "codebuild:ListFleets",
        "codecommit:Get*",
        "codeconnections:GetConnection",
```

```
        "codeconnections:List*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:List*",
        "codepipeline:Get*",
        "codepipeline:List*",
        "codestar-connections:Get*",
        "codestar-connections:List*",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:ListNotificationRules",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:Get*",
        "cognito-identity:ListIdentityPools",
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:GetStoredQuery",
        "config:List*",
        "connect-campaigns:Describe*",
        "connect-campaigns:List*",
        "controltower:Get*",
        "controltower:List*",
        "cur:Describe*",
        "cur:ListTagsForResource",
        "databrew:Describe*",
        "databrew:List*",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datasync:Describe*",
        "datasync:List*",
        "deadline:Get*",
        "deadline:List*",
        "detective:Describe*",
        "detective:GetMembers",
        "detective:List*",
        "devicefarm:Get*",
        "devicefarm:List*",
        "devops-guru:Describe*",
        "devops-guru:Get*",
```

```
        "devops-guru:List*",
        "directconnect:Describe*",
        "dms:Describe*",
        "dms:List*",
        "ds:Describe*",
        "ds:ListTagsForResource",
        "dsql:Get*",
        "dsql:List*",
        "ecr-public:Describe*",
        "ecr-public:Get*",
        "ecr-public:ListTagsForResource",
        "ecr:Describe*",
        "ecr:Get*",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
        "eks:List*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:List*",
        "elemental-inference:GetFeed",
        "elemental-inference:List*",
        "emr-containers:Describe*",
        "emr-containers:List*",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "entityresolution:Get*",
        "entityresolution:List*",
        "events:Describe*",
        "events:List*",
        "evidently:GetSegment",
        "evidently:List*",
        "evs:GetEnvironment",
        "evs:List*",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:List*",
        "fis:Get*",
```

```
        "fis:List*",
        "fms:Get*",
        "fms:List*",
        "forecast:Describe*",
        "forecast:List*",
        "fsx:Describe*",
        "gamelift:Describe*",
        "gamelift:List*",
        "gamelift:ValidateMatchmakingRuleSet",
        "gameliftstreams:Get*",
        "gameliftstreams:List*",
        "geo:Describe*",
        "geo:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "grafana:Describe*",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetDeployment",
        "greengrass:List*",
        "groundstation:Get*",
        "groundstation:List*",
        "guardduty:DescribePublishingDestination",
        "guardduty:Get*",
        "guardduty:List*",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:List*",
        "iam:Get*",
        "iam:List*",
        "imagebuilder:Get*",
        "imagebuilder:List*",
        "inspector:Describe*",
        "inspector:List*",
        "inspector2:Get*",
        "inspector2:List*",
        "interconnect:GetConnection",
        "interconnect:List*",
        "internetmonitor:Get*",
        "internetmonitor:List*",
        "invoicing:GetInvoiceUnit",
        "invoicing:List*",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
```

```
        "iotanalytics:Describe*",
        "iotanalytics:List*",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:Describe*",
        "iotevents:List*",
        "iotfleetwise:Get*",
        "iotfleetwise:List*",
        "iotsitewise:Describe*",
        "iotsitewise:List*",
        "iottwinmaker:Get*",
        "iottwinmaker:List*",
        "iotwireless:Get*",
        "iotwireless:List*",
        "ivs:Get*",
        "ivs:List*",
        "ivschat:Get*",
        "ivschat:List*",
        "kafka-cluster:Describe*",
        "kafka:Describe*",
        "kafka:Get*",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra-ranking:DescribeRescoreExecutionPlan",
        "kendra-ranking:List*",
        "kendra:Describe*",
        "kendra:List*",
        "kinesis:Describe*",
        "kinesis:List*",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kinesisvideo:List*",
        "lakeformation:Describe*",
        "lakeformation:GetLFTag",
        "lakeformation:List*",
        "lambda:GetFunctionConcurrency",
        "launchwizard:GetDeployment",
        "launchwizard:List*",
        "lex:Describe*",
        "lex:GetBotAlias",
        "lex:List*",
        "license-manager:Get*",
```

```
        "license-manager:List*",
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListInferenceSchedulers",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:Get*",
        "m2:List*",
        "macie2:Get*",
        "macie2:List*",
        "managedblockchain:GetAccessor",
        "managedblockchain:ListAccessors",
        "mediaconnect:Describe*",
        "mediaconnect:Get*",
        "mediaconnect:List*",
        "medialive:Describe*",
        "medialive:Get*",
        "medialive:List*",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:Get*",
        "mediapackagev2:List*",
        "mediatailor:Describe*",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:List*",
        "medical-imaging:GetDatastore",
        "medical-imaging:List*",
        "mobiletargeting:Get*",
        "mobiletargeting:List*",
        "mpa:Get*",
        "mpa:List*",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:Describe*",
        "network-firewall:List*",
        "networkmanager:Describe*",
        "networkmanager:Get*",
        "networkmanager:List*",
        "nimble:GetStudio",
        "nimble:ListStudios",
```

```
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:List*",
        "notifications:Get*",
        "notifications:List*",
        "nova-act:GetWorkflowDefinition",
        "nova-act:ListWorkflowDefinitions",
        "oam:Get*",
        "oam:List*",
        "observabilityadmin:Get*",
        "observabilityadmin:List*",
        "odb:Get*",
        "odb:List*",
        "omics:Get*",
        "omics:List*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:Get*",
        "osis:List*",
        "panorama:Describe*",
        "panorama:List*",
        "payment-cryptography:Get*",
        "payment-cryptography:List*",
        "pca-connector-ad:Get*",
        "pca-connector-ad:List*",
        "pca-connector-scep:Get*",
        "pca-connector-scep:List*",
        "pcs:Get*",
        "pcs:List*",
        "personalize:Describe*",
        "personalize:List*",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "profile:Get*",
        "profile:List*",
        "proton:Get*",
        "proton:List*",
        "qbusiness:Get*",
        "qbusiness:List*",
        "quicksight:Describe*",
        "quicksight:List*",
        "ram:Get*",
        "ram:List*",
        "rbin:GetRule",
        "rbin:List*",
```

```
        "refactor-spaces:Get*",
        "refactor-spaces:List*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resiliencehub:Describe*",
        "resiliencehub:Get*",
        "resiliencehub:List*",
        "resource-explorer-2:Get*",
        "resource-explorer-2:List*",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:SearchResources",
        "robomaker:Describe*",
        "robomaker:List*",
        "rolesanywhere:Get*",
        "rolesanywhere:List*",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53profiles:Get*",
        "route53profiles:List*",
        "route53resolver:Get*",
        "route53resolver:List*",
        "rtbfabric:Get*",
        "rtbfabric:List*",
        "rum:BatchGetRumMetricDefinitions",
        "rum:Get*",
        "rum:List*",
        "sagemaker:Describe*",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:List*",
        "sagemaker:ListMonitoringSchedules",
        "scheduler:Get*",
        "scheduler:List*",
        "schemas:Describe*",
        "schemas:List*",
        "securitylake:Get*",
        "securitylake:List*",
        "servicecatalog:Describe*",
        "servicecatalog:Get*",
        "servicecatalog:List*",
```

```
        "ses:Describe*",
        "ses:Get*",
        "ses:List*",
        "shield:Describe*",
        "shield:List*",
        "signer:Get*",
        "signer:List*",
        "simspaceweaver:DescribeSimulation",
        "simspaceweaver:ListSimulations",
        "sms-voice:Describe*",
        "sms-voice:Get*",
        "sms-voice:List*",
        "sns:Get*",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:List*",
        "ssm-contacts:Get*",
        "ssm-contacts:List*",
        "ssm-guiconnect:Get*",
        "ssm-incidents:Get*",
        "ssm-incidents:List*",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:GetApplication",
        "ssm-sap:List*",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "states:Describe*",
        "states:List*",
        "supportapp:Get*",
        "supportapp:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "tag:GetResources",
        "thinclient:GetEnvironment",
        "thinclient:List*",
        "transfer:Describe*",
        "transfer:List*",
        "trustedadvisor:GetRecommendation",
        "trustedadvisor:ListChecks",
        "trustedadvisor:ListRecommendationResources",
        "trustedadvisor:ListRecommendations",
```

```
        "trustedadvisor:ListRecommendationsForResource",
        "verifiedpermissions:Get*",
        "verifiedpermissions:List*",
        "voiceid:DescribeDomain",
        "voiceid:List*",
        "vpc-lattice:Get*",
        "vpc-lattice:List*",
        "wafv2:Get*",
        "wafv2:List*",
        "wisdom:Get*",
        "wisdom:List*",
        "workspaces-instances:Get*",
        "workspaces-instances:List*",
        "workspaces-web:Get*",
        "workspaces-web:List*",
        "workspaces:Describe*",
        "xray:Get*",
        "xray:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudControlDiscoveryCompactExact",
      "Effect" : "Allow",
      "Action" : [
        "aoss:BatchGetCollection",
        "aoss:BatchGetCollectionGroup",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollectionGroups",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "appsync:GetApi",
        "appsync:GetChannelNamespace",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
```

```
        "appsync:GetGraphqlApi",
        "appsync:GetSourceApiAssociation",
        "appsync:ListApis",
        "appsync:ListChannelNamespaces",
        "appsync:ListDataSources",
        "appsync:ListDomainNames",
        "appsync:ListFunctions",
        "appsync:ListGraphqlApis",
        "appsync:ListResolvers",
        "appsync:ListSourceApiAssociations",
        "appsync:ListTagsForResource",
        "cases:BatchGetCaseRule",
        "cases:BatchGetField",
        "cases:GetDomain",
        "cases:GetLayout",
        "cases:GetTemplate",
        "cases:ListCaseRules",
        "cases:ListDomains",
        "cases:ListFields",
        "cases:ListLayouts",
        "cases:ListTemplates",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribePublisher",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
        "cloudformation:ListTypeVersions",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeTerms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
```

```
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTerms",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "connect:DescribeAgentStatus",
        "connect:DescribeContactFlow",
        "connect:DescribeContactFlowModule",
        "connect:DescribeContactFlowModuleAlias",
        "connect:DescribeDataTable",
        "connect:DescribeEvaluationForm",
        "connect:DescribeHoursOfOperation",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribeNotification",
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUserHierarchyGroup",
        "connect:DescribeView",
        "connect:DescribeWorkspace",
        "connect:GetTaskTemplate",
        "connect:ListAgentStatuses",
        "connect:ListApprovedOrigins",
        "connect:ListBots",
        "connect:ListContactFlowModuleAliases",
        "connect:ListContactFlowModules",
        "connect:ListContactFlowModuleVersions",
        "connect:ListContactFlows",
        "connect:ListContactFlowVersions",
        "connect:ListDataTableAttributes",
        "connect:ListDataTables",
        "connect:ListEvaluationForms",
        "connect:ListEvaluationFormVersions",
        "connect:ListHoursOfOperationOverrides",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
```

```
        "connect:ListIntegrationAssociations",
        "connect:ListLambdaFunctions",
        "connect:ListNotifications",
        "connect:ListPredefinedAttributes",
        "connect:ListPrompts",
        "connect:ListQueueEmailAddresses",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileManualAssignmentQueues",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfileFlowModules",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListTrafficDistributionGroups",
        "connect:ListUserHierarchyGroups",
        "connect:ListUserProficiencies",
        "connect:ListUsers",
        "connect:ListViews",
        "connect:ListViewVersions",
        "connect:ListWorkspaceMedia",
        "connect:ListWorkspacePages",
        "connect:ListWorkspaces",
        "connect:SearchWorkspaceAssociations",
        "datazone:GetDataSource",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentProfile",
        "datazone:GetGroupProfile",
        "datazone:GetProject",
        "datazone:GetProjectProfile",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListDataSources",
```

```
        "datazone:ListDomains",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjectProfiles",
        "datazone:ListProjects",
        "datazone:ListSubscriptionTargets",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAwsNetworkPerformanceMetricSubscriptions",
        "ec2:DescribeCapacityManagerDataExports",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeHosts",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceConnectEndpoints",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstances",
```

```
        "ec2:DescribeInstanceSqlHaStates",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpamPrefixListResolvers",
        "ec2:DescribeIpamPrefixListResolverTargets",
        "ec2:DescribeIpamResourceDiscoveries",
        "ec2:DescribeIpamResourceDiscoveryAssociations",
        "ec2:DescribeIpams",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteServerEndpoints",
        "ec2:DescribeRouteServerPeers",
        "ec2:DescribeRouteServers",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilterRules",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayMeteringPolicies",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
```

```
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstanceLoggingConfigurations",
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:DescribeVpcEncryptionControls",
        "ec2:DescribeVpcEndpointAssociations",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConcentrators",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetIpamPrefixListResolverRules",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetRouteServerAssociations",
        "ec2:GetRouteServerPropagations",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayMeteringPolicyEntries",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:SearchTransitGatewayRoutes",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSubnetGroups",
```

```
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeServerlessCaches",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "es:GetApplication",
        "es:ListApplications",
        "es:ListTags",
        "frauddetector:BatchGetVariable",
        "frauddetector:DescribeDetector",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "glue:DescribeIntegrations",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetCrawler",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetIntegrationResourceProperty",
        "glue:GetJob",
        "glue:GetRegistry",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetUsageProfile",
        "glue:ListCrawlers",
        "glue:ListIntegrationResourceProperties",
        "glue:ListJobs",
        "glue:ListRegistries",
        "glue:ListSchemas",
        "glue:ListSchemaVersions",
        "glue:ListTriggers",
```

```
        "glue:ListUsageProfiles",
        "identitystore:DescribeGroup",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "kms:DescribeCustomKeyStores",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:GetParametersForImport",
        "kms:GetPublicKey",
        "kms:ListAliases",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeyRotations",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "kms:ListRetirableGrants",
        "lambda:GetAlias",
        "lambda:GetCapacityProvider",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionScalingConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListCapacityProviders",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctions",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "lightsail:GetAlarms",
```

```
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "memorydb:DescribeACLs",
        "memorydb:DescribeClusters",
        "memorydb:DescribeMultiRegionClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "neptune-graph:GetGraph",
        "neptune-graph:GetGraphSnapshot",
        "neptune-graph:GetPrivateGraphEndpoint",
        "neptune-graph:ListGraphs",
        "neptune-graph:ListGraphSnapshots",
        "neptune-graph:ListPrivateGraphEndpoints",
        "neptune-graph:ListTagsForResource",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListTagsForResource",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
```

```
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterDbRevisions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "route53globalresolver:GetAccessSource",
        "route53globalresolver:GetDNSView",
        "route53globalresolver:GetFirewallDomainList",
        "route53globalresolver:GetFirewallRule",
        "route53globalresolver:GetGlobalResolver",
        "route53globalresolver:GetHostedZoneAssociation",
        "route53globalresolver:ListAccessSources",
        "route53globalresolver:ListAccessTokens",
```

```
        "route53globalresolver:ListDNSViews",
        "route53globalresolver:ListFirewallDomainLists",
        "route53globalresolver:ListFirewallRules",
        "route53globalresolver:ListGlobalResolvers",
        "route53globalresolver:ListHostedZoneAssociations",
        "route53globalresolver:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
```

```
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetObjectAcl",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3:ListTagsForResource",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetAccessPointScope",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetInventoryConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:GetMetricsConfiguration",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListTagsForResource",
        "s3files:GetAccessPoint",
        "s3files:GetFileSystem",
        "s3files:GetFileSystemPolicy",
        "s3files:GetMountTarget",
        "s3files:GetSynchronizationConfiguration",
        "s3files:ListAccessPoints",
        "s3files:ListFileSystems",
        "s3files:ListMountTargets",
        "s3files:ListTagsForResource",
        "s3tables:GetNamespace",
        "s3tables:GetTable",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketMetricsConfiguration",
        "s3tables:GetTableBucketPolicy",
```

```
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:GetTableMaintenanceConfiguration",
        "s3tables:GetTablePolicy",
        "s3tables:GetTableStorageClass",
        "s3tables:ListNamespaces",
        "s3tables:ListTableBuckets",
        "s3tables:ListTables",
        "s3tables:ListTagsForResource",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:ListIndexes",
        "s3vectors:ListTagsForResource",
        "s3vectors:ListVectorBuckets",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "securityagent:BatchGetAgentSpaces",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetTargetDomains",
        "securityagent:GetApplication",
        "securityagent:ListAgentSpaces",
        "securityagent:ListApplications",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentests",
        "securityagent:ListTagsForResource",
        "securityagent:ListTargetDomains",
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetSecurityControls",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeSecurityHubV2",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetAggregatorV2",
        "securityhub:GetAutomationRuleV2",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetConnectorV2",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:GetInsights",
        "securityhub:ListAggregatorsV2",
        "securityhub:ListAutomationRules",
```

```
        "securityhub:ListAutomationRulesV2",
        "securityhub:ListConfigurationPolicies",
        "securityhub:ListConfigurationPolicyAssociations",
        "securityhub:ListConnectorsV2",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:ListFindingAggregators",
        "securityhub:ListOrganizationAdminAccounts",
        "securityhub:ListSecurityControlDefinitions",
        "securityhub:ListTagsForResource",
        "ssm:DescribeAssociation",
        "ssm:DescribeDocument",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeMaintenanceWindowTargets",
        "ssm:DescribeMaintenanceWindowTasks",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetMaintenanceWindow",
        "ssm:GetMaintenanceWindowTask",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso-directory:DescribeGroup",
        "sso-directory:SearchGroups",
        "sts:GetCallerIdentity",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeScheduledQuery",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListScheduledQueries",
        "timestream:ListTables",
        "timestream:ListTagsForResource"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

WellArchitectedConsoleFullAccess

Descrição: Fornece acesso total à AWS Well-Architected ferramenta por meio do Console de gerenciamento da AWS

`WellArchitectedConsoleFullAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `WellArchitectedConsoleFullAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2018, 18:19 UTC
- Horário editado: 09 de julho de 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wellarchitected:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "agent.wellarchitected.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "trustedadvisor:List*",
        "trustedadvisor:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:*:iam::*:role/aws-service-role/*/
AWSServiceRoleForWellArchitected*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "wellarchitected.amazonaws.com",
            "agent.wellarchitected.amazonaws.com",
            "metrics.wellarchitected.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:*:iam::*:role/aws-service-role/*/
AWSServiceRoleForWellArchitected*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion"
      ],
```

```
      "Resource" : "arn:aws:iam::*:policy/service-role/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "wellarchitected.amazonaws.com",
            "agent.wellarchitected.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

WellArchitectedConsoleReadOnlyAccess

Descrição: Fornece acesso somente para leitura à AWS Well-Architected Ferramenta por meio do Console de gerenciamento da AWS

`WellArchitectedConsoleReadOnlyAccess` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `WellArchitectedConsoleReadOnlyAccess` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 29 de novembro de 2018, 18:21 UTC
- Horário editado: 09 de julho de 2026, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*",
        "wellarchitected:ExportLens",
        "organizations:DescribeAccount",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
```

```
        "trustedadvisor:List*",
        "trustedadvisor:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

WorkLinkServiceRolePolicy

Descrição: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pela Amazon WorkLink

`WorkLinkServiceRolePolicy` é uma política gerenciada pelo AWS.

Utilização desta política

Você pode vincular a `WorkLinkServiceRolePolicy` aos seus usuários, grupos e perfis.

Detalhes desta política

- Tipo: política AWS gerenciada
- Hora da criação: 23 de janeiro de 2019, 19:03 UTC
- Hora da edição: 23 de janeiro de 2019, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy`

Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com a política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se permite a solicitação.

Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/AmazonWorkLink-*"
    }
  ]
}
```

Saiba mais

- Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center
- Adicionar e remover permissões de identidade IAM
- Compreenda o controle de versionamento das políticas do IAM
- Comece com políticas AWS gerenciadas e avance para permissões com privilégios mínimos

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.